109TH CONGRESS } HOUSE OF REPRESENTATIVES { REPT. 109–71
1st Session } { Part 2

DEPARTMENT OF HOMELAND SECURITY AUTHORIZATION ACT FOR FISCAL YEAR 2006

MAY 13, 2005.—Ordered to be printed

Mr. BARTON of Texas, from the Committee on Energy and Commerce, submitted the following

R E P O R T

[To accompany H.R. 1817]

[Including cost estimate of the Congressional Budget Office]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 1817) to authorize appropriations for fiscal year 2006 for the Department of Homeland Security, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

AMENDMENT

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Department of Homeland Security Authorization Act for Fiscal Year 2006".

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

TITLE I—AUTHORIZATION OF APPROPRIATIONS

SEC. 101. DEPARTMENT OF HOMELAND SECURITY.

There is authorized to be appropriated to the Secretary of Homeland Security for the necessary expenses of the Department of Homeland Security for fiscal year 2006, $34,152,143,000.

SEC. 102. BORDER PATROL AGENTS.

Of the amount authorized under section 101, there is authorized to be appropriated for fiscal year 2006 for border security and control between ports of entry, including for the hiring of 2,000 border patrol agents in addition to the number employed on the date of enactment of this Act, and related training and support costs, $1,916,427,000.

SEC. 103. DEPARTMENTAL MANAGEMENT AND OPERATIONS.

Of the amount authorized under section 101, there is authorized to be appropriated for fiscal year 2006 for departmental management and operations, $634,687,000, of which—

(1) $44,895,000 is authorized for the Department of Homeland Security Regions Initiative;

(2) $4,459,000 is authorized for Operation Integration Staff; and

(3) $56,278,000 is authorized for Office of Security initiatives.

SEC. 104. CRITICAL INFRASTRUCTURE GRANTS.

Of the amount authorized under section 101, there is authorized to be appropriated for fiscal year 2006 for grants and other assistance to improve critical infrastructure protection, $500,000,000.

SEC. 105. RESEARCH AND DEVELOPMENT.

Of the amount authorized under section 101, there are authorized to be appropriated for fiscal year 2006—

(1) $76,573,000 to support chemical countermeasure development activities of the Directorate of Science and Technology;

(2) $197,314,000 to support a nuclear detection office and related activities of such directorate;

(3) $10,000,000 for research and development of technologies capable of countering threats posed by man-portable air defense systems, including location-based technologies and noncommercial aircraft-based technologies; and

(4) $10,600,000 for the activities of such directorate conducted pursuant to subtitle G of title VIII of the Homeland Security Act of 2002 (6 U.S.C. 441 et seq.).

SEC. 106. BORDER AND TRANSPORTATION SECURITY.

Of the amount authorized under section 101, there are authorized to be appropriated for fiscal year 2006—

(1) $826,913,000 for expenses related to Screening Coordination and Operations of the Directorate of Border and Transportation Security;

(2) $100,000,000 for weapons of mass destruction detection technology of such directorate; and

(3) $133,800,000 for the Container Security Initiative of such directorate.

SEC. 107. STATE AND LOCAL TERRORISM PREPAREDNESS.

Of the amount authorized under section 101, there is authorized to be appropriated for fiscal year 2006—

(1) $40,500,000 for the activities of the Office for Interoperability and Compatibility within the Directorate of Science and Technology pursuant to section 7303 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C 194); and

(2) $1,000,000,000 for discretionary grants for high-threat, high-density urban areas awarded by the Office of State and Local Government Coordination and Preparedness.

SEC. 108. AUTHORIZATION OF APPROPRIATIONS FOR TRAINING OF STATE AND LOCAL PERSONNEL IN BORDER STATES PERFORMING IMMIGRATION FUNCTIONS.

(a) IN GENERAL.—To carry out subsection (b), subject to such limitations as may be provided in Acts making appropriations for Management and Administration for U.S. Immigration and Customs Enforcement, there are authorized to be appropriated from such amounts $40,000,000 for fiscal year 2006, to remain available

until September 30, 2007, for the purpose of enhancing the integrity of the border security system of the United States against the threat of terrorism.

(b) USE OF FUNDS.—From amounts made available under subsection (a), the Secretary of Homeland Security may reimburse a State or political subdivision described in subsection (c) for the expenses described in subsection (d).

(c) ELIGIBLE RECIPIENTS.—A State, or a political subdivision of a State, is eligible for reimbursement under subsection (b) if the State or political subdivision—

(1) contains a location that is 30 miles or less from a border or coastline of the United States;

(2) has entered into a written agreement described in section 287(g) of the Immigration and Nationality Act (8 U.S.C. 1357(g)) under which certain officers or employees of the State or subdivision may be authorized to perform certain functions of an immigration officer; and

(3) desires such officers or employees to receive training from the Department of Homeland Security in relation to such functions.

(d) EXPENSES.—The expenses described in this subsection are actual and necessary expenses incurred by the State or political subdivision in order to permit the training described in subsection (c)(3) to take place, including expenses such as the following:

(1) Costs of travel and transportation to locations where training is provided, including mileage and related allowances for the use of a privately owned automobile.

(2) Subsistence consisting of lodging, meals, and other necessary expenses for the personal sustenance and comfort of a person required to travel away from the person's regular post of duty in order to participate in the training.

(3) A per diem allowance paid instead of actual expenses for subsistence and fees or tips to porters and stewards.

(4) Costs of securing temporary replacements for personnel traveling to, and participating in, the training.

SEC. 109. METROPOLITAN MEDICAL RESPONSE SYSTEM.

Of the amount authorized under section 101, there is authorized to be appropriated $75,000,000 for fiscal year 2006 for the Metropolitan Medical Response System.

TITLE II—TERRORISM PREVENTION, INFORMATION SHARING, AND RISK ASSESSMENT

Subtitle A—Terrorism Prevention

SEC. 201. TERRORISM PREVENTION PLAN AND RELATED BUDGET SUBMISSION.

(a) DEPARTMENT OF HOMELAND SECURITY TERRORISM PREVENTION PLAN.—

(1) REQUIREMENTS.—Not later than 1 year after the date of enactment of the Act, and on a regular basis thereafter, the Secretary of Homeland Security shall prepare and submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a Department of Homeland Security Terrorism Prevention Plan. The Plan shall be a comprehensive and integrated plan that includes the goals, objectives, milestones, and key initiatives of the Department of Homeland Security to prevent acts of terrorism on the United States, including its territories and interests.

(2) CONTENTS.—The Secretary shall include in the Plan the following elements:

(A) Identification and prioritization of groups and subgroups that pose the most significant threat of committing acts of terrorism on the United States and its interests.

(B) Identification of the most significant current, evolving, and long-term terrorist threats to the United States and its interests, including an evaluation of—

(i) the materials that may be used to carry out a potential attack;

(ii) the methods that may be used to carry out a potential attack; and

(iii) the outcome the perpetrators of acts of terrorism aim to achieve.

(C) A prioritization of the threats identified under subparagraph (B), based on an assessment of probability and consequence of such attacks.

(D) A description of processes and procedures that the Secretary shall establish to institutionalize close coordination between the Department of

Homeland Security and the National Counter Terrorism Center and other appropriate United States intelligence agencies.

(E) The policies and procedures the Secretary shall establish to ensure the Department gathers real-time information from the National Counter Terrorism Center; disseminates this information throughout the Department, as appropriate; utilizes this information to support the Department's counterterrorism responsibilities; integrates the Department's information collection and analysis functions; and disseminates this information to its operational units, as appropriate.

(F) A description of the specific actions the Secretary shall take to identify threats of terrorism on the United States and its interests, and to coordinate activities within the Department to prevent acts of terrorism, with special emphasis on prevention of terrorist access to and use of weapons of mass destruction.

(G) A description of initiatives the Secretary shall take to share critical terrorism prevention information with, and provide terrorism prevention support to, State and local governments and the private sector.

(H) A timeline, with goals and milestones, for implementing the Homeland Security Information Network, the Homeland Security Secure Data Network, and other departmental information initiatives to prevent acts of terrorism on the United States and its interests, including integration of these initiatives in the operations of the Homeland Security Operations Center.

(I) Such other terrorism prevention-related elements as the Secretary considers appropriate.

(3) CONSULTATION.—In formulating the Plan the Secretary shall consult with—

(A) the Director of National Intelligence;

(B) the Director of the National Counter Terrorism Center;

(C) the Attorney General;

(D) the Director of the Federal Bureau of Investigation;

(E) the Secretary of Defense;

(F) the Secretary of State;

(G) the Secretary of Energy;

(H) the Secretary of the Treasury; and

(I) the heads of other Federal agencies and State, county, and local law enforcement agencies as the Secretary considers appropriate.

(4) CLASSIFICATION.—The Secretary shall prepare the Plan in both classified and nonclassified forms.

(b) ANNUAL CROSSCUTTING ANALYSIS OF PROPOSED FUNDING FOR DEPARTMENT OF HOMELAND SECURITY PROGRAMS.—

(1) REQUIREMENT TO SUBMIT ANALYSIS.—The Secretary of Homeland Security shall submit to the Congress, concurrently with the submission of the President's budget for each fiscal year, a detailed, crosscutting analysis of the budget proposed for the Department of Homeland Security, by budget function, by agency, and by initiative area, identifying the requested amounts of gross and net appropriations or obligational authority and outlays for programs and activities of the Department for each of the following mission areas:

(A) To prevent terrorist attacks within the United States.

(B) To reduce the vulnerability of the United States to terrorism.

(C) To minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States.

(D) To carry out all functions of the agencies and subdivisions within the Department that are not related directly to homeland security.

(2) FUNDING ANALYSIS OF MULTIPURPOSE FUNCTIONS.—The analysis required under paragraph (1) for functions that are both related directly and not related directly to homeland security shall include a detailed allocation of funding for each specific mission area within those functions, including an allocation of funding among mission support functions, such as agency overhead, capital assets, and human capital.

(3) INCLUDED TERRORISM PREVENTION ACTIVITIES.—The analysis required under paragraph (1)(A) shall include the following activities (among others) of the Department:

(A) Collection and effective use of intelligence and law enforcement operations that screen for and target individuals who plan or intend to carry out acts of terrorism.

(B) Investigative, intelligence, and law enforcement operations that identify and disrupt plans for acts of terrorism or reduce the ability of groups or individuals to commit acts of terrorism.

(C) Investigative activities and intelligence operations to detect and prevent the introduction of weapons of mass destruction into the United States.

(D) Initiatives to detect potential, or the early stages of actual, biological, chemical, radiological, or nuclear attacks.

(E) Screening individuals against terrorist watch lists.

(F) Screening cargo to identify and segregate high-risk shipments.

(G) Specific utilization of information sharing and intelligence, both horizontally (within the Federal Government) and vertically (among Federal, State, and local governments), to detect or prevent acts of terrorism.

(H) Initiatives, including law enforcement and intelligence operations, to preempt, disrupt, and deter acts of terrorism overseas intended to strike the United States.

(I) Investments in technology, research and development, training, and communications systems that are designed to improve the performance of the Department and its agencies with respect to each of the activities listed in subparagraphs (A) through (H).

(4) SEPARATE DISPLAYS FOR MANDATORY AND DISCRETIONARY AMOUNTS.—Each analysis under paragraph (1) shall include separate displays for proposed mandatory appropriations and proposed discretionary appropriations.

SEC. 202. CONSOLIDATED BACKGROUND CHECK PROCESS.

(a) REQUIREMENT.—The Secretary shall establish a single process for conducting the security screening and background checks on individuals participating in any voluntary or mandatory departmental credentialing or registered traveler program.

(b) INCLUDED PROGRAMS.—The process established under subsection (a) shall be sufficient to meet the security requirements of all applicable Departmental programs, including—

(1) the Transportation Worker Identification Credential;

(2) the Hazmat Endorsement Credential;

(3) the Free and Secure Trade program;

(4) the NEXUS and SENTRI border crossing programs;

(5) the Registered Traveler program of the Transportation Security Administration; and

(6) any other similar program or credential considered appropriate for inclusion by the Secretary.

(c) FEATURES OF PROCESS.—The process established under subsection (a) shall include the following:

(1) A single submission of security screening information, including personal data and biometric information as appropriate, necessary to meet the security requirements of all applicable departmental programs.

(2) An ability to submit such security screening information at any location or through any process approved by the Secretary with respect to any of the applicable departmental programs.

(3) Acceptance by the Department of a security clearance issued by a Federal agency, to the extent that the security clearance process of the agency satisfies requirements that are at least as stringent as those of the applicable departmental programs under this section.

(4) Standards and procedures for protecting individual privacy, confidentiality, record retention, and addressing other concerns relating to information security.

(d) DEADLINES.—The Secretary of Homeland Security shall—

(1) submit a description of the process developed under subsection (a) to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate by not later than 6 months after the date of the enactment of this Act; and

(2) begin implementing such process by not later than 12 months after the date of the enactment of this Act.

(e) RELATIONSHIP TO OTHER LAWS.—(1) Nothing in this section affects any statutory requirement relating to the operation of the programs described in subsection (b).

(2) Nothing in this section affects any statutory requirement relating to title III of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 435b et seq.).

Subtitle B—Homeland Security Information Sharing and Analysis Enhancement

SEC. 211. SHORT TITLE.

This subtitle may be cited as the "Homeland Security Information Sharing and Analysis Enhancement Act of 2005".

SEC. 212. PROVISION OF TERRORISM-RELATED INFORMATION TO PRIVATE SECTOR OFFICIALS.

Section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is amended by adding at the end the following:

"(20) To require, in consultation with the Assistant Secretary for Infrastructure Protection, the creation and routine dissemination of analytic reports and products designed to provide timely and accurate information that has specific relevance to each of the Nation's critical infrastructure sectors (as identified in the national infrastructure protection plan issued under paragraph (5)), to private sector officials in each such sector who are responsible for protecting institutions within that sector from potential acts of terrorism and for mitigating the potential consequences of any such act.".

SEC. 213. ANALYTIC EXPERTISE ON THE THREATS FROM BIOLOGICAL AGENTS AND NUCLEAR WEAPONS.

Section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is further amended by adding at the end the following:

"(21) To ensure sufficient analytic expertise within the Office of Information Analysis to create and disseminate, on an ongoing basis, products based on the analysis of homeland security information, as defined in section 892(f)(1), with specific reference to the threat of terrorism involving the use of nuclear weapons and biological agents to inflict mass casualties or other catastrophic consequences on the population or territory of the United States.".

SEC. 214. ALTERNATIVE ANALYSIS OF HOMELAND SECURITY INFORMATION.

(a) REQUIREMENT.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended by adding at the end the following:

"SEC. 203. ALTERNATIVE ANALYSIS OF HOMELAND SECURITY INFORMATION.

"The Secretary shall establish a process and assign an individual or entity the responsibility to ensure that, as appropriate, elements of the Department conduct alternative analysis (commonly referred to as 'red-team analysis') of homeland security information, as that term is defined in section 892(f)(1), that relates to potential acts of terrorism involving the use of nuclear weapons or biological agents to inflict mass casualties or other catastrophic consequences on the population or territory of the United States.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the item relating to section 202 the following:

"Sec. 203. Alternative analysis of homeland security information.".

SEC. 215. ASSIGNMENT OF INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION FUNCTIONS.

Section 201(b) of the Homeland Security Act of 2002 (6 U.S.C. 121(b)) is amended by adding at the end the following:

"(4) ASSIGNMENT OF SPECIFIC FUNCTIONS.—The Under Secretary for Information Analysis and Infrastructure Protection—

"(A) shall assign to the Assistant Secretary for Information Analysis the responsibility for performing the functions described in paragraphs (1), (4), (7) through (14), (16), and (18) of subsection (d);

"(B) shall assign to the Assistant Secretary for Infrastructure Protection the responsibility for performing the functions described in paragraphs (2), (5), and (6) of subsection (d);

"(C) shall ensure that the Assistant Secretary for Information Analysis and the Assistant Secretary for Infrastructure Protection both perform the functions described in paragraphs (3), (15), (17), and (19) of subsection (d);

"(D) may assign to each such Assistant Secretary such other duties relating to such responsibilities as the Under Secretary may provide;

"(E) shall direct each such Assistant Secretary to coordinate with Federal, State, and local law enforcement agencies, and with tribal and private sector entities, as appropriate; and

"(F) shall direct the Assistant Secretary for Information Analysis to coordinate with elements of the intelligence community, as appropriate.".

SEC. 216. AUTHORITY FOR DISSEMINATING HOMELAND SECURITY INFORMATION.

(a) IN GENERAL.—Title I of the Homeland Security Act of 2002 (6 U.S.C. 111 et seq.) is amended by adding at the end the following:

"SEC. 104. AUTHORITY FOR DISSEMINATING HOMELAND SECURITY INFORMATION.

"(a) PRIMARY AUTHORITY.—Except as provided in subsection (b), the Secretary shall be the executive branch official responsible for disseminating homeland security information to State and local government and tribal officials and the private sector.

"(b) PRIOR APPROVAL REQUIRED.—No Federal official may disseminate any homeland security information, as defined in section 892(f)(1), to State, local, tribal, or private sector officials without the Secretary's prior approval, except—

"(1) in exigent circumstances under which it is essential that the information be communicated immediately; or

"(2) when such information is issued to State, local, or tribal law enforcement officials for the purpose of assisting them in any aspect of the administration of criminal justice.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the item relating to section 103 the following:

"Sec. 104. Authority for disseminating homeland security information.".

SEC. 217. 9/11 MEMORIAL HOMELAND SECURITY FELLOWS PROGRAM.

(a) ESTABLISHMENT OF PROGRAM.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is further amended by adding at the end the following:

"SEC. 204. 9/11 MEMORIAL HOMELAND SECURITY FELLOWS PROGRAM.

"(a) ESTABLISHMENT.—

"(1) IN GENERAL.—The Secretary shall establish a fellowship program in accordance with this section for the purpose of bringing State, local, tribal, and private sector officials to participate in the work of the Homeland Security Operations Center in order to become familiar with—

"(A) the mission and capabilities of that Center; and

"(B) the role, programs, products, and personnel of the Office of Information Analysis, the Office of Infrastructure Protection, and other elements of the Department responsible for the integration, analysis, and dissemination of homeland security information, as defined in section 892(f)(1).

"(2) PROGRAM NAME.—The program under this section shall be known as the 9/11 Memorial Homeland Security Fellows Program.

"(b) ELIGIBILITY.—In order to be eligible for selection as a fellow under the program, an individual must—

"(1) have homeland security-related responsibilities; and

"(2) possess an appropriate national security clearance.

"(c) LIMITATIONS.—The Secretary—

"(1) may conduct up to 4 iterations of the program each year, each of which shall be 90 days in duration; and

"(2) shall ensure that the number of fellows selected for each iteration does not impede the activities of the Center.

"(d) CONDITION.—As a condition of selecting an individual as a fellow under the program, the Secretary shall require that the individual's employer agree to continue to pay the individual's salary and benefits during the period of the fellowship.

"(e) STIPEND.—During the period of the fellowship of an individual under the program, the Secretary shall, subject to the availability of appropriations—

"(1) provide to the individual a stipend to cover the individual's reasonable living expenses during the period of the fellowship; and

"(2) reimburse the individual for round-trip, economy fare travel to and from the individual's place of residence twice each month.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by adding at the end of the items relating to such subtitle the following:

"Sec. 204. 9/11 Memorial Homeland Security Fellows Program.".

SEC. 218. ACCESS TO NUCLEAR TERRORISM-RELATED INFORMATION.

Section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is further amended by adding at the end the following:

"(22) To ensure that—

"(A) the Assistant Secretary for Information Analysis receives promptly and without request all information obtained by any component of the Department if that information relates, directly or indirectly, to a threat of terrorism involving the potential use of nuclear weapons;

"(B) such information is—

"(i) integrated and analyzed comprehensively; and

"(ii) disseminated in a timely manner, including to appropriately cleared State, local, tribal, and private sector officials; and

"(C) such information is used to determine what requests the Department should submit for collection of additional information relating to that threat.".

SEC. 219. ACCESS OF ASSISTANT SECRETARY FOR INFORMATION ANALYSIS TO TERRORISM INFORMATION.

Section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is further amended by adding at the end the following:

"(23) To ensure that the Assistant Secretary for Information Analysis—

"(A) is routinely and without request given prompt access to all terrorism-related information collected by or otherwise in the possession of any component of the Department, including all homeland security information (as that term is defined in section 892(f)(1)); and

"(B) to the extent technologically feasible has direct access to all databases of any component of the Department that may contain such information.".

SEC. 220. ADMINISTRATION OF THE HOMELAND SECURITY INFORMATION NETWORK.

Section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is further amended by adding at the end the following:

"(24) To administer the homeland security information network, including—

"(A) exercising primary responsibility for establishing a secure nationwide real-time homeland security information sharing network for Federal, State, and local government agencies and authorities, tribal officials, the private sector, and other governmental and private entities involved in receiving, analyzing, and distributing information related to threats to homeland security;

"(B) ensuring that the information sharing systems, developed in connection with the network established under subparagraph (A), are utilized and are compatible with, to the greatest extent practicable, Federal, State, and local government, tribal, and private sector antiterrorism systems and protocols that have been or are being developed; and

"(C) ensuring, to the greatest extent possible, that the homeland security information network and information systems are integrated and interoperable with existing private sector technologies.".

SEC. 221. IAIP PERSONNEL RECRUITMENT.

(a) IN GENERAL.—Chapter 97 of title 5, United States Code, is amended by adding after section 9701 the following:

"§ 9702. Recruitment bonuses

"(a) IN GENERAL.—Notwithstanding any provision of chapter 57, the Secretary of Homeland Security, acting through the Under Secretary for Information Analysis and Infrastructure Protection, may pay a bonus to an individual in order to recruit such individual for a position that is primarily responsible for discharging the analytic responsibilities specified in section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) and that—

"(1) is within the Directorate for Information Analysis and Infrastructure Protection; and

"(2) would be difficult to fill in the absence of such a bonus.

In determining which individuals are to receive bonuses under this section, appropriate consideration shall be given to the Directorate's critical need for linguists.

"(b) BONUS AMOUNT, FORM, ETC.—

"(1) IN GENERAL.—The amount of a bonus under this section shall be determined under regulations of the Secretary of Homeland Security, but may not exceed 50 percent of the annual rate of basic pay of the position involved.

"(2) FORM OF PAYMENT.—A bonus under this section shall be paid in the form of a lump-sum payment and shall not be considered to be part of basic pay.

"(3) COMPUTATION RULE.—For purposes of paragraph (1), the annual rate of basic pay of a position does not include any comparability payment under section 5304 or any similar authority.

"(c) SERVICE AGREEMENTS.—Payment of a bonus under this section shall be contingent upon the employee entering into a written service agreement with the Department of Homeland Security. The agreement shall include—

"(1) the period of service the individual shall be required to complete in return for the bonus; and

"(2) the conditions under which the agreement may be terminated before the agreed-upon service period has been completed, and the effect of any such termination.

"(d) ELIGIBILITY.—A bonus under this section may not be paid to recruit an individual for—

"(1) a position to which an individual is appointed by the President, by and with the advice and consent of the Senate;

"(2) a position in the Senior Executive Service as a noncareer appointee (as defined under section 3132(a)); or

"(3) a position which has been excepted from the competitive service by reason of its confidential, policy-determining, policy-making, or policy-advocating character.

"(e) TERMINATION.—The authority to pay bonuses under this section shall terminate on September 30, 2008.

"§ 9703. Reemployed annuitants

"(a) IN GENERAL.—If an annuitant receiving an annuity from the Civil Service Retirement and Disability Fund becomes employed in a position within the Directorate for Information Analysis and Infrastructure Protection of the Department of Homeland Security, the annuitant's annuity shall continue. An annuitant so reemployed shall not be considered an employee for the purposes of chapter 83 or 84.

"(b) TERMINATION.—The exclusion pursuant to this section of the Directorate for Information Analysis and Infrastructure Protection from the reemployed annuitant provisions of chapters 83 and 84 shall terminate 3 years after the date of the enactment of this section, unless extended by the Secretary of Homeland Security. Any such extension shall be for a period of 1 year and shall be renewable.

"(c) ANNUITANT DEFINED.—For purposes of this section, the term 'annuitant' has the meaning given such term under section 8331 or 8401, whichever is appropriate.

"§ 9704. Regulations

"The Secretary of Homeland Security, in consultation with the Director of the Office of Personnel Management, may prescribe any regulations necessary to carry out section 9702 or 9703.".

(b) CLERICAL AMENDMENT.—The analysis for chapter 97 of title 5, United States Code, is amended by adding after the item relating to section 9701 the following:

"9702. Recruitment bonuses.
"9703. Reemployed annuitants.
"9704. Regulations.".

SEC. 222. INFORMATION COLLECTION REQUIREMENTS AND PRIORITIES.

(a) IN GENERAL.—Section 102 of the Homeland Security Act of 2002 (6 U.S.C. 112) is amended—

(1) by redesignating subsections (e), (f), and (g), as subsections (f), (g), and (h), respectively; and

(2) by inserting after subsection (d) the following new subsection (e):

"(e) PARTICIPATION IN FOREIGN COLLECTION REQUIREMENTS AND MANAGEMENT PROCESSES.—The Secretary shall be a member of any Federal Government interagency board, established by Executive order or any other binding interagency directive, that is responsible for establishing foreign collection information requirements and priorities for estimative analysis.".

(b) HOMELAND SECURITY INFORMATION REQUIREMENTS BOARD.—

(1) IN GENERAL.—Title I of such Act (6 U.S.C. 111 et seq.) is further amended by adding at the end the following new section:

"SEC. 105. HOMELAND SECURITY INFORMATION REQUIREMENTS BOARD.

"(a) ESTABLISHMENT OF BOARD.—There is established an interagency Homeland Security Information Requirements Board (hereinafter in this section referred to as the 'Information Requirements Board').

"(b) MEMBERSHIP.—The following officials are members of the Information Requirements Board:

"(1) The Secretary of Homeland Security, who shall serve as the Chairman of the Information Requirements Board.

"(2) The Attorney General.

"(3) The Secretary of Commerce.

"(4) The Secretary of the Treasury.

"(5) The Secretary of Defense.

"(6) The Secretary of Energy.

"(7) The Secretary of State.

"(8) The Secretary of the Interior.

"(9) The Director of National Intelligence.

"(10) The Director of the Federal Bureau of Investigation.

"(11) The Director of the National Counterterrorism Center.

"(12) The Chief Privacy Officer of the Department of Homeland Security.

"(c) FUNCTIONS.—

"(1) OVERSIGHT OF HOMELAND SECURITY REQUIREMENTS.—The Information Requirements Board shall oversee the process for establishing homeland security requirements and collection management for all terrorism-related information and all other homeland security information (as defined in section 892(f)(1)) collected within the United States.

"(2) DETERMINATION OF COLLECTION PRIORITIES.—The Information Requirements Board shall—

"(A) determine the domestic information collection requirements for information relevant to the homeland security mission; and

"(B) prioritize the collection and use of such information.

"(3) COORDINATION OF COLLECTION REQUIREMENTS AND MANAGEMENT ACTIVITIES.—

"(A) COORDINATION WITH COUNTERPART AGENCIES.—The Chairman shall ensure that the Information Requirements Board carries out its activities in a manner that is fully coordinated with the Board's counterpart entities.

"(B) PARTICIPATION OF COUNTERPART ENTITIES.—The Chairman and the Director of National Intelligence shall ensure that each counterpart entity—

"(i) has at least one representative on the Information Requirement Board and on every subcomponent of the Board; and

"(ii) meets jointly with the Information Requirements Board (and, as appropriate, with any subcomponent of the Board) as often as the Chairman and the Director of National Intelligence determine appropriate.

"(C) COUNTERPART ENTITY DEFINED.—In this section, the term 'counterpart entity' means an entity of the Federal Government that is responsible for foreign intelligence collection requirements and management.

"(d) MEETINGS.—

"(1) IN GENERAL.—The Information Requirements Board shall meet regularly at such times and places as its Chairman may direct.

"(2) INVITED REPRESENTATIVES.—The Chairman may invite representatives of Federal agencies not specified in subsection (b) to attend meetings of the Information Requirements Board.".

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by inserting after the item relating to section 104 the following new item:

"Sec. 105. Homeland Security Information Requirements Board.".

SEC. 223. HOMELAND SECURITY ADVISORY SYSTEM.

(a) IN GENERAL.—Subtitle A of title II of the Homeland Security Act of 2002 is further amended—

(1) in section 201(d)(7) (6 U.S.C. 121(d)(7)) by inserting "under section 205" after "System"; and

(2) by adding at the end the following:

"SEC. 205. HOMELAND SECURITY ADVISORY SYSTEM.

"(a) REQUIREMENT.—The Under Secretary for Information Analysis and Infrastructure Protection shall implement a Homeland Security Advisory System in accordance with this section to provide public advisories and alerts regarding threats to homeland security, including national, regional, local, and economic sector advisories and alerts, as appropriate.

"(b) REQUIRED ELEMENTS.—The Under Secretary, under the System—

"(1) shall include, in each advisory and alert regarding a threat, information on appropriate protective measures and countermeasures that may be taken in response to the threat;

"(2) shall, whenever possible, limit the scope of each advisory and alert to a specific region, locality, or economic sector believed to be at risk; and

"(3) shall not, in issuing any advisory or alert, use color designations as the exclusive means of specifying the homeland security threat conditions that are the subject of the advisory or alert.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by adding at the end of the items relating to subtitle A of title II the following:

"Sec. 205. Homeland Security Advisory System.".

SEC. 224. USE OF OPEN-SOURCE INFORMATION.

Section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) is further amended by adding at the end the following:

"(25) To ensure that, whenever possible—

"(A) the Assistant Secretary for Information Analysis produces and disseminates reports and analytic products based on open-source information that do not require a national security classification under applicable law; and

"(B) such unclassified open-source reports are produced and disseminated contemporaneously with reports or analytic products concerning the same or similar information that the Assistant Secretary for Information Analysis produces and disseminates in a classified format.".

SEC. 225. FULL AND EFFICIENT USE OF OPEN-SOURCE INFORMATION.

(a) REQUIREMENT.—Subtitle A of title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is further amended by adding at the end the following:

"SEC. 206. FULL AND EFFICIENT USE OF OPEN-SOURCE INFORMATION.

"The Under Secretary shall ensure that, in meeting their analytic responsibilities under section 201(d) and in formulating requirements for collection of additional information, the Assistant Secretary for Information Analysis and the Assistant Secretary for Infrastructure Protection make full and efficient use of open-source information wherever possible.".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is further amended by inserting after the item relating to section 205 the following:

"Sec. 206. Full and efficient use of open-source information.".

TITLE III—DOMESTIC PREPAREDNESS AND PROTECTION

Subtitle A—Preparedness and Protection

SEC. 301. NATIONAL TERRORISM EXERCISE PROGRAM.

(a) IN GENERAL.—Section 430(c) of the Homeland Security Act of 2002 (6 U.S.C. 238) is amended by striking "and" after the semicolon at the end of paragraph (8), by striking the period at the end of paragraph (9) and inserting "; and", and by adding at the end the following:

"(10) designing, developing, performing, and evaluating exercises at the national, State, territorial, regional, local, and tribal levels of government that incorporate government officials, emergency response providers, public safety agencies, the private sector, international governments and organizations, and other appropriate entities to test the Nation's capability to prevent, prepare for, respond to, and recover from threatened or actual acts of terrorism.".

(b) NATIONAL TERRORISM EXERCISE PROGRAM.—

(1) ESTABLISHMENT OF PROGRAM.—Title VIII of the Homeland Security Act of 2002 (Public Law 107–296) is amended by adding at the end the following new subtitle:

"Subtitle J—Terrorism Preparedness Exercises

"SEC. 899a. NATIONAL TERRORISM EXERCISE PROGRAM.

"(a) IN GENERAL.—The Secretary, through the Office for Domestic Preparedness, shall establish a National Terrorism Exercise Program for the purpose of testing and evaluating the Nation's capabilities to prevent, prepare for, respond to, and recover from threatened or actual acts of terrorism that—

"(1) enhances coordination for terrorism preparedness between all levels of government, emergency response providers, international governments and organizations, and the private sector;

"(2) is—

"(A) multidisciplinary in nature, including, as appropriate, information analysis and cybersecurity components;

"(B) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;

"(C) carried out with the minimum degree of notice to involved parties regarding the timing and details of such exercises, consistent with safety considerations;

"(D) evaluated against performance measures and followed by corrective action to solve identified deficiencies; and

"(E) assessed to learn best practices, which shall be shared with appropriate Federal, State, territorial, regional, local, and tribal personnel, authorities, and training institutions for emergency response providers; and

"(3) assists State, territorial, local, and tribal governments with the design, implementation, and evaluation of exercises that—

"(A) conform to the requirements of paragraph (2); and

"(B) are consistent with any applicable State homeland security strategy or plan.

"(b) NATIONAL LEVEL EXERCISES.—The Secretary, through the National Terrorism Exercise Program, shall perform on a periodic basis national terrorism preparedness exercises for the purposes of—

"(1) involving top officials from Federal, State, territorial, local, tribal, and international governments, as the Secretary considers appropriate;

"(2) testing and evaluating the Nation's capability to detect, disrupt, and prevent threatened or actual catastrophic acts of terrorism, especially those involving weapons of mass destruction; and

"(3) testing and evaluating the Nation's readiness to respond to and recover from catastrophic acts of terrorism, especially those involving weapons of mass destruction.

"(c) CONSULTATION WITH FIRST RESPONDERS.—In implementing the responsibilities described in subsections (a) and (b), the Secretary shall consult with a geographic (including urban and rural) and substantive cross section of governmental and nongovernmental first responder disciplines, including as appropriate—

"(1) Federal, State, and local first responder training institutions;

"(2) representatives of emergency response providers; and

"(3) State and local officials with an expertise in terrorism preparedness.".

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by adding at the end of the items relating to title VIII the following:

"Subtitle J—Terrorism Preparedness Exercises

"Sec. 899a. National terrorism exercise program.".

(c) TOPOFF PREVENTION EXERCISE.—No later than one year after the date of enactment of this Act, the Secretary of Homeland Security shall design and carry out a national terrorism prevention exercise for the purposes of—

(1) involving top officials from Federal, State, territorial, local, tribal, and international governments; and

(2) testing and evaluating the Nation's capability to detect, disrupt, and prevent threatened or actual catastrophic acts of terrorism, especially those involving weapons of mass destruction.

SEC. 302. TECHNOLOGY DEVELOPMENT AND TRANSFER.

(a) ESTABLISHMENT OF TECHNOLOGY CLEARINGHOUSE.—Not later than 90 days after the date of enactment of this Act, the Secretary shall complete the establishment of the Technology Clearinghouse under section 313 of the Homeland Security Act of 2002.

(b) TRANSFER PROGRAM.—Section 313 of the Homeland Security Act of 2002 (6 U.S.C. 193) is amended—

(1) by adding at the end of subsection (b) the following new paragraph:

"(6) The establishment of a homeland security technology transfer program to facilitate the identification, modification, and commercialization of technology and equipment for use by Federal, State, and local governmental agencies, emergency response providers, and the private sector to prevent, prepare for, or respond to acts of terrorism.";

(2) by redesignating subsection (c) as subsection (d); and

(3) by inserting after subsection (b) the following new subsection:

"(c) TECHNOLOGY TRANSFER PROGRAM.—In developing the program described in subsection (b)(6), the Secretary, acting through the Under Secretary for Science and Technology, shall—

"(1) in consultation with the other Under Secretaries of the Department and the Director of the Office for Domestic Preparedness, on an ongoing basis—

"(A) conduct surveys and reviews of available appropriate technologies that have been, or are in the process of being developed, tested, evaluated, or demonstrated by the Department, other Federal agencies, or the private sector or foreign governments and international organizations and that may

be useful in assisting Federal, State, and local governmental agencies, emergency response providers, or the private sector to prevent, prepare for, or respond to acts of terrorism;

"(B) conduct or support research, development, tests, and evaluations, as appropriate of technologies identified under subparagraph (A), including any necessary modifications to such technologies for antiterrorism use;

"(C) communicate to Federal, State, and local governmental agencies, emergency response providers, or the private sector the availability of such technologies for antiterrorism use, as well as the technology's specifications, satisfaction of appropriate standards, and the appropriate grants available from the Department to purchase such technologies;

"(D) coordinate the selection and administration of all technology transfer activities of the Science and Technology Directorate, including projects and grants awarded to the private sector and academia; and

"(E) identify priorities based on current risk assessments within the Department of Homeland Security for identifying, researching, developing, testing, evaluating, modifying, and fielding existing technologies for antiterrorism purposes;

"(2) in support of the activities described in paragraph (1)—

"(A) consult with Federal, State, and local emergency response providers;

"(B) consult with government agencies and nationally recognized standards development organizations as appropriate;

"(C) enter into agreements and coordinate with other Federal agencies, foreign governments, and national and international organizations as the Secretary determines appropriate, in order to maximize the effectiveness of such technologies or to facilitate commercialization of such technologies; and

"(D) consult with existing technology transfer programs and Federal and State training centers that research, develop, test, evaluate, and transfer military and other technologies for use by emergency response providers; and

"(3) establish a working group in coordination with the Secretary of Defense to advise and assist the technology clearinghouse in the identification of military technologies that are in the process of being developed, or are developed, by the Department of Defense or the private sector, which may include—

"(A) representatives from the Department of Defense or retired military officers;

"(B) nongovernmental organizations or private companies that are engaged in the research, development, testing, or evaluation of related technologies or that have demonstrated prior experience and success in searching for and identifying technologies for Federal agencies;

"(C) Federal, State, and local emergency response providers; and

"(D) to the extent the Secretary considers appropriate, other organizations, other interested Federal, State, and local agencies, and other interested persons.".

(c) REPORT.—Not later than 1 year after the date of enactment of this Act, the Under Secretary for Science and Technology shall transmit to the Committees on Homeland Security and Energy and Commerce of the House of Representatives and the Committees on Homeland Security and Governmental Affairs and Commerce, Science, and Transportation of the Senate a description of the progress the Department has made in implementing the provisions of section 313 of the Homeland Security Act of 2002, as amended by this Act, including a description of the process used to review unsolicited proposals received as described in subsection (b)(3) of such section.

(d) SAVINGS CLAUSE.—Nothing in this section (including the amendments made by this section) shall be construed to alter or diminish the effect of the limitation on the authority of the Secretary of Homeland Security under section 302(4) of the Homeland Security Act of 2002 (6 U.S.C. 182(4)) with respect to human health-related research and development activities.

SEC. 303. REVIEW OF ANTITERRORISM ACQUISITIONS.

(a) STUDY.—The Secretary of Homeland Security shall conduct a study of all Department of Homeland Security procurements, including ongoing procurements and anticipated procurements, to—

(1) identify those that involve any product, equipment, service (including support services), device, or technology (including information technology) that is being designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause; and

(2) assess whether such product, equipment, service (including support services), device, or technology is an appropriate candidate for the litigation and risk management protections of subtitle G of title VIII of the Homeland Security Act of 2002.

(b) SUMMARY AND CLASSIFICATION REPORT.—Not later than 180 days after the date of enactment of this Act, the Secretary shall transmit to the Congress a report—

(1) describing each product, equipment, service (including support services), device, and technology identified under subsection (a) that the Secretary believes would be an appropriate candidate for the litigation and risk management protections of subtitle G of title VIII of the Homeland Security Act of 2002;

(2) listing each such product, equipment, service (including support services), device, and technology in order of priority for deployment in accordance with current terrorism risk assessment information; and

(3) setting forth specific actions taken, or to be taken, to encourage or require persons or entities that sell or otherwise provide such products, equipment, services (including support services), devices, and technologies to apply for the litigation and risk management protections of subtitle G of title VIII of the Homeland Security Act of 2002, and to ensure prioritization of the Department's review of such products, equipment, services, devices, and technologies under such Act in accordance with the prioritization set forth in paragraph (2) of this subsection.

SEC. 304. CENTER OF EXCELLENCE FOR BORDER SECURITY.

The Secretary of Homeland Security shall establish a university-based Center for Excellence for Border Security following the merit-review processes and procedures that have been established for selecting University Programs Centers of Excellence. The Center shall prioritize its activities on the basis of risk to address the most significant threats, vulnerabilities, and consequences posed by the Nation's borders and border control systems, including the conduct of research, the examination of existing and emerging border security technology and systems, and the provision of education, technical, and analytical assistance for the Department of Homeland Security to effectively secure the Nation's borders.

SEC. 305. REQUIREMENTS RELATING TO THE CONTAINER SECURITY INITIATIVE (CSI).

(a) RISK ASSESSMENT AND DESIGNATION OF NEW FOREIGN SEAPORTS.—

(1) RISK ASSESSMENT.—The Secretary of Homeland Security shall conduct a risk assessment of each foreign seaport that the Secretary is considering designating as a port under the Container Security Initiative (CSI) on or after the date of the enactment of this Act. Each such assessment shall evaluate the level of risk for the potential compromise of cargo containers by terrorists or terrorist weapons.

(2) DESIGNATION.—The Secretary is authorized to designate a foreign seaport as a port under CSI on or after the date of the enactment of this Act only if the Secretary determines, based on a risk assessment under paragraph (1) and a cost-benefit analysis, that the benefits of designating such port outweigh the cost of expanding the program to such port.

(b) DEPLOYMENT OF INSPECTION EQUIPMENT TO NEW CSI PORTS.—

(1) DEPLOYMENT.—The Secretary is authorized to assist in the loaning of nonintrusive inspection equipment for cargo containers, on a nonreimbursable basis, at each CSI port designated under subsection (a)(2) and provide training for personnel at the CSI port to operate the nonintrusive inspection equipment.

(2) ADDITIONAL REQUIREMENTS.—The Secretary shall establish technical capability requirements and standard operating procedures for nonintrusive inspection equipment described in paragraph (1) and shall require each CSI port to agree to operate such equipment in accordance with such requirements and procedures as a condition for receiving the equipment and training under such paragraph.

(c) DEPLOYMENT OF PERSONNEL TO NEW CSI PORTS; REEVALUATION OF PERSONNEL AT ALL CSI PORTS.—

(1) DEPLOYMENT.—The Secretary shall deploy Department of Homeland Security personnel to each CSI port designated under subsection (a)(1) with respect to which the Secretary determines that the deployment is necessary to successfully implement the requirements of CSI at the port.

(2) REEVALUATION.—The Secretary shall periodically review relevant risk assessment information with respect to all CSI ports at which Department of Homeland Security personnel are deployed to assess whether or not continued deployment of such personnel, in whole or in part, is necessary to successfully implement the requirements of CSI at the port.

(d) INSPECTION AND SCREENING AT UNITED STATES PORTS OF ENTRY.—Cargo containers arriving at a United States port of entry from a CSI port shall undergo the same level of inspection and screening for potential compromise by terrorists or terrorist weapons as cargo containers arriving at a United States port of entry from a foreign seaport that is not participating in CSI unless the containers were initially inspected at the CSI port at the request of CSI personnel and such personnel verify and electronically record that the inspection indicates that the containers have not been compromised by terrorists or terrorist weapons.

(e) DEFINITION.—In this section, the term "Container Security Initiative" or "CSI" means the program carried out by the Department of Homeland Security under which the Department enters into agreements with foreign seaports to—

(1) establish security criteria to identify high-risk maritime cargo containers bound for the United States based on advance information; and

(2) screen or inspect such maritime cargo containers for potential compromise by terrorists or terrorist weapons prior to shipment to the United States.

SEC. 306. SECURITY OF MARITIME CARGO CONTAINERS.

(a) REGULATIONS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall issue regulations for the security of maritime cargo containers moving within the intermodal transportation system in accordance with the requirements of paragraph (2).

(2) REQUIREMENTS.—The regulations issued pursuant to paragraph (1) shall be in accordance with recommendations of the Maritime Transportation Security Act Subcommittee of the Advisory Committee on Commercial Operations of the Department of Homeland Security, including recommendations relating to obligation to seal, recording of seal changes, modal changes, seal placement, ocean carrier seal verification, and addressing seal anomalies.

(b) INTERNATIONAL AGREEMENTS.—The Secretary shall seek to enter into agreements with foreign countries and international organizations to establish standards for the security of maritime cargo containers moving within the intermodal transportation system that, to the maximum extent practicable, meet the requirements of subsection (a)(2).

(c) CONTAINER TARGETING STRATEGY.—

(1) STRATEGY.—The Secretary shall develop a strategy to improve the ability of the Department of Homeland Security to use information contained in shipping bills of lading to identify and provide additional review of anomalies in such bills of lading. The strategy shall include a method of contacting shippers in a timely fashion to verify or explain any anomalies in shipping bills of lading.

(2) REPORT.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall submit to the Committees on Homeland Security and Energy and Commerce of the House of Representatives and the Committees on Homeland Security and Governmental Affairs and Commerce, Science, and Transportation of the Senate a report on the implementation of this subsection, including information on any data searching technologies that will be used to implement the strategy.

(d) CONTAINER SECURITY DEMONSTRATION PROGRAM.—

(1) PROGRAM.—The Secretary is authorized to establish and carry out a demonstration program that integrates nonintrusive inspection equipment, including radiation detection equipment and gamma ray inspection equipment, at an appropriate United States seaport, as determined by the Secretary.

(2) REQUIREMENT.—The demonstration program shall also evaluate automatic identification methods for containers and vehicles and a data sharing network capable of transmitting inspection data between ports and appropriate entities within the Department of Homeland Security.

(3) REPORT.—Upon completion of the demonstration program, the Secretary shall submit to the Committees on Homeland Security and Energy and Commerce of the House of Representatives and the Committees on Homeland Security and Governmental Affairs and Commerce, Science, and Transportation of the Senate a report on the implementation of this subsection.

(e) CONSOLIDATION OF CONTAINER SECURITY PROGRAMS.—The Secretary shall consolidate all programs of the Department of Homeland Security relating to the security of maritime cargo containers, including the demonstration program established pursuant to subsection (d), to achieve enhanced coordination and efficiency.

SEC. 307. SECURITY PLAN FOR GENERAL AVIATION AT RONALD REAGAN WASHINGTON NATIONAL AIRPORT.

Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security shall implement section 823(a) of the Vision 100—Century of Aviation Reauthorization Act (49 U.S.C. 41718 note; 117 Stat. 2595).

SEC. 308. INTEROPERABLE COMMUNICATIONS ASSISTANCE.

(a) FINDINGS.—The Congress finds the following:

(1) The 9/11 Commission determined that the inability of first responders to communicate effectively on September 11, 2001 was a critical obstacle to an effective multi-jurisdictional response.

(2) Many jurisdictions across the country still experience difficulties communicating that may contribute to confusion, delays, or added risks when responding to an emergency.

(3) During fiscal year 2004, the Office for Domestic Preparedness awarded over $834,000,000 for 2,912 projects through Department of Homeland Security grant programs for the purposes of improving communications interoperability.

(4) Interoperable communications systems are most effective when designed to comprehensively address, on a regional basis, the communications of all types of public safety agencies, first responder disciplines, and State and local government facilities.

(5) Achieving communications interoperability is complex due to the extensive training, system modifications, and agreements among the different jurisdictions that are necessary to implement effective communications systems.

(6) The Congress authorized the Department of Homeland Security to create an Office for Interoperability and Compatibility in the Intelligence Reform and Terrorism Prevention Act of 2004 to, among other things, establish a comprehensive national approach, coordinate federal activities, accelerate the adoption of standards, and encourage research and development to achieve interoperable communications for first responders.

(7) The Office for Interoperability and Compatibility includes the SAFECOM Program that serves as the umbrella program within the Federal government to improve public safety communications interoperability, and has developed the RAPIDCOM program, the Statewide Communications Interoperability Planning Methodology, and a Statement of Requirements to provide technical, planning, and purchasing assistance for Federal departments and agencies, State and local governments, and first responders.

(b) SENSE OF CONGRESS.—It is the sense of the Congress that the Department of Homeland Security should implement as expeditiously as possible the initiatives assigned to the Office for Interoperability and Compatibility under section 7303 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 194), including specifically the following:

(1) Establishing a comprehensive national approach to achieving public safety interoperable communications.

(2) Issuing letters of intent to commit future funds for jurisdictions through existing homeland security grant programs to applicants as appropriate to encourage long-term investments that may significantly improve communications interoperability.

(3) Providing technical assistance to additional urban and other high-risk areas to support the establishment of consistent, secure, and effective interoperable communications capabilities.

(4) Completing the report to the Congress on the Department's plans for accelerating the development of national voluntary consensus standards for public safety interoperable communications, a schedule of milestones for such development, and achievements of such development, by no later than 30 days after the date of enactment of this Act.

SEC. 309. REPORT TO CONGRESS ON IMPLEMENTATION OF RECOMMENDATIONS REGARDING PROTECTION OF AGRICULTURE.

The Secretary of Homeland Security shall report to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate by no later than 120 days after the date of the enactment of this Act regarding how the Department of Homeland Security will implement the applicable recommendations from the Government Accountability Office report entitled "Homeland Security: Much is Being Done to Protect Agriculture from a Terrorist Attack, but Important Challenges Remain" (GAO–05–214).

Subtitle B—Department of Homeland Security Cybersecurity Enhancement

SEC. 311. SHORT TITLE.

This subtitle may be cited as the "Department of Homeland Security Cybersecurity Enhancement Act of 2005".

SEC. 312. ASSISTANT SECRETARY FOR CYBERSECURITY.

(a) ESTABLISHMENT.—Section 201(b) of the Homeland Security Act of 2002 (6 U.S.C. 121(b)) is amended—

(1) by redesignating paragraph (3) as paragraph (4); and

(2) by inserting after paragraph (2) the following new paragraph:

"(3) ASSISTANT SECRETARY FOR CYBERSECURITY.—There shall be in the Department an Assistant Secretary for Cybersecurity, who shall be appointed by the President."; and

(3) in paragraph (4), as redesignated by subparagraph (A) of this paragraph—

(A) by striking "Analysis and the" and inserting "Analysis, the" and

(B) by striking "Protection shall" and inserting "Protection, and the Assistant Secretary for Cybersecurity shall".

(b) RESPONSIBILITIES.—The Under Secretary of Information Analysis and Infrastructure Protection shall assign to the Assistant Secretary for Cybersecurity responsibility for—

(1) the National Cyber Security Division and the National Communications System within the Department of Homeland Security;

(2) the cybersecurity-related aspects of paragraphs (2), (3), (5), (6), (15), and (17) of subsection (d) of section 201 of the Homeland Security Act of 2002; and

(3) such other duties as the Under Secretary may provide pursuant to section 201 of such Act.

(c) COORDINATION.—The Assistant Secretary of Cybersecurity shall coordinate all activities under this subtitle with other Federal agencies, including the Department of Commerce, the Department of Energy, the Department of Transportation, the Federal Communications Commission, the Nuclear Regulatory Commission, the Federal Energy Regulatory Commission, the Environmental Protection Agency, the Federal Trade Commission, and the National Telecommunications and Information Administration.

SEC. 313. CYBERSECURITY DEFINED.

For the purposes of this subtitle, the term "cybersecurity" means the protection and restoration of networked electronic equipment and facilities, including hardware and software and the information contained therein, from intrusion, interference, and incapacitation.

SEC. 314. CYBERSECURITY TRAINING PROGRAMS AND EQUIPMENT.

(a) IN GENERAL.—The Secretary of Homeland Security, acting through the Assistant Secretary for Cybersecurity, may establish, in conjunction with the National Science Foundation, a program to award grants to institutions of higher education (and consortia thereof) for—

(1) the establishment or expansion of cybersecurity professional development programs;

(2) the establishment or expansion of associate degree programs in cybersecurity; and

(3) the purchase of equipment to provide training in cybersecurity for either professional development programs or degree programs.

(b) ROLES.—

(1) DEPARTMENT OF HOMELAND SECURITY.—The Secretary, acting through the Assistant Secretary for Cybersecurity and in consultation with the Director of the National Science Foundation, shall establish the goals for the program established under this section and the criteria for awarding grants under the program.

(2) NATIONAL SCIENCE FOUNDATION.—The Director of the National Science Foundation shall operate the program established under this section consistent with the goals and criteria established under paragraph (1), including soliciting applicants, reviewing applications, and making and administering grant awards. The Director may consult with the Assistant Secretary for Cybersecurity in selecting awardees.

(3) FUNDING.—The Secretary shall transfer to the National Science Foundation the funds necessary to carry out this section.

(c) GRANT AWARDS.—

(1) PEER REVIEW.—All grant awards under this section shall be made on a competitive, merit-reviewed basis.

(2) FOCUS.—In making grant awards under this section, the Director shall, to the extent practicable, ensure geographic diversity and the participation of women and underrepresented minorities.

(3) PREFERENCE.—In making grant awards under this section, the Director shall give preference to applications submitted by consortia of institutions to encourage as many students and professionals as possible to benefit from this program.

(d) AUTHORIZATION OF APPROPRIATIONS.—Of the amount authorized under section 101, there is authorized to be appropriated to the Secretary for carrying out this section $3,700,000 for fiscal year 2006.

(e) DEFINITIONS.—In this section, the term "institution of higher education" has the meaning given that term in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a)).

Subtitle C—Security of Public Transportation Systems

SEC. 321. SECURITY BEST PRACTICES.

Not later than 120 days after the date of enactment of this Act, the Secretary of Homeland Security shall develop, disseminate to appropriate owners, operators, and providers of public transportation systems, public transportation employees and employee representatives, and Federal, State, and local officials, and transmit to Congress, a report containing best practices for the security of public transportation systems. In developing best practices, the Secretary shall be responsible for consulting with and collecting input from owners, operators, and providers of public transportation systems, public transportation employee representatives, first responders, industry associations, private sector experts, academic experts, and appropriate Federal, State, and local officials.

SEC. 322. PUBLIC AWARENESS.

Not later than 90 days after the date of enactment of this Act, the Secretary of Homeland Security shall develop a national plan for public outreach and awareness. Such plan shall be designed to increase awareness of measures that the general public, public transportation passengers, and public transportation employees can take to increase public transportation system security. Such plan shall also provide outreach to owners, operators, providers, and employees of public transportation systems to improve their awareness of available technologies, ongoing research and development efforts, and available Federal funding sources to improve public transportation security. Not later than 9 months after the date of enactment of this Act, the Secretary shall implement the plan developed under this section.

Subtitle D—Critical Infrastructure Prioritization

SEC. 331. CRITICAL INFRASTRUCTURE.

(a) COMPLETION OF PRIORITIZATION.—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security shall complete the prioritization of the Nation's critical infrastructure according to all of the following criteria:

(1) The threat of terrorist attack, based on threat information received and analyzed by the Office of Information Analysis of the Department regarding the intentions and capabilities of terrorist groups and other potential threats to the Nation's critical infrastructure.

(2) The likelihood that an attack would cause the destruction or significant disruption of such infrastructure.

(3) The likelihood that an attack would result in substantial numbers of deaths and serious bodily injuries, a substantial adverse impact on the national economy, or a substantial adverse impact on national security.

(b) COOPERATION.—Such prioritization shall be developed in cooperation with other relevant Federal agencies, State, local, and tribal governments, and the private sector, as appropriate. The Secretary shall coordinate the prioritization under this section with other Federal agencies, including the Department of Commerce, the Department of Energy, the Department of Transportation, the Federal Communications Commission, the Nuclear Regulatory Commission, the Federal Energy Regulatory Commission, the Environmental Protection Agency, the Federal Trade Commission, and the National Telecommunications and Information Administration.

SEC. 332. SECURITY REVIEW.

(a) REQUIREMENT.—Not later than 9 months after the date of the enactment of this Act, the Secretary, in coordination with other relevant Federal agencies, State, local, and tribal governments, and the private sector, as appropriate, shall—

(1) review existing Federal, State, local, tribal, and private sector plans for securing the critical infrastructure included in the prioritization developed under section 331;

(2) recommend changes to existing plans for securing such infrastructure, as the Secretary determines necessary; and

(3) coordinate and contribute to protective efforts of other Federal, State, local, and tribal agencies and the private sector, as appropriate, as directed in Homeland Security Presidential Directive 7.

(b) CONTENTS OF PLANS.—The recommendations made under subsection (a)(2) shall include—

(1) necessary protective measures to secure such infrastructure, including milestones and timeframes for implementation; and

(2) to the extent practicable, performance metrics to evaluate the benefits to both national security and the Nation's economy from the implementation of such protective measures.

(c) COORDINATION.—The Secretary shall coordinate the security review and recommendations required by subsection (a) with other Federal agencies, including the Department of Commerce, the Department of Energy, the Department of Transportation, the Federal Communications Commission, the Nuclear Regulatory Commission, the Federal Energy Regulatory Commission, the Environmental Protection Agency, the Federal Trade Commission, and the National Telecommunications and Information Administration.

SEC. 333. IMPLEMENTATION REPORT.

(a) IN GENERAL.—Not later than 15 months after the date of the enactment of this Act, the Secretary shall submit a report to the Committees on Homeland Security and Energy and Commerce of the House of Representatives and the Committees on Homeland Security and Governmental Affairs and Commerce, Science, and Transportation of the Senate on the implementation of section 332. Such report shall detail—

(1) the Secretary's review and coordination of security plans under section 332; and

(2) the Secretary's oversight of the execution and effectiveness of such plans.

(b) UPDATE.—Not later than 1 year after the submission of the report under subsection (a), the Secretary, following the coordination required by section 332(c), shall provide an update of such report to the congressional committees described in subsection (a).

SEC. 334. PROTECTION OF INFORMATION.

Information that is generated, compiled, or disseminated by the Department of Homeland Security in carrying out this section—

(1) is exempt from disclosure under section 552 of title 5, United States Code; and

(2) shall not, if provided by the Department to a State or local government or government agency—

(A) be made available pursuant to any State or local law requiring disclosure of information or records;

(B) otherwise be disclosed or distributed to any person by such State or local government or government agency without the written consent of the Secretary; or

(C) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act.

TITLE IV—MISCELLANEOUS

SEC. 401. BORDER SECURITY AND ENFORCEMENT COORDINATION AND OPERATIONS.

(a) FINDINGS.—The Congress makes the following findings:

(1) In creating the Department of Homeland Security, the Congress sought to enhance the Nation's capabilities to prevent, protect against, and respond to terrorist acts by consolidating existing Federal agencies with homeland security functions into a single new Department, and by realigning the missions of those legacy agencies to more directly support our national homeland security efforts.

(2) As part of this massive government reorganization, section 442 of the Homeland Security Act of 2002 (Public Law 107–273) established a Bureau of Border Security and transferred into it all of the functions, programs, personnel, assets, and liabilities pertaining to the following programs: the Border Patrol; alien detention and removal; immigration-related intelligence, investigations, and enforcement activities; and immigration inspections at ports of entry.

(3) Title IV of the Homeland Security Act of 2002 (Public Law 107–273) also transferred to the new Department the United States Customs Service, as a dis-

tinct entity within the new Department, to further the Department's border integrity mission.

(4) Utilizing its reorganization authority provided in the Homeland Security Act of 2002, the President submitted a reorganization plan for the Department on January 30, 2003.

(5) This plan merged the customs and immigration border inspection and patrol functions, along with agricultural inspections functions, into a new entity called United States Customs and Border Protection.

(6) The plan also combined the customs and immigration enforcement agents, as well as the Office of Detention and Removal Operations, the Office of Federal Protective Service, the Office of Federal Air Marshal Service, and the Office of Intelligence, into another new entity called United States Immigration and Customs Enforcement.

(7) The President's January 30, 2003, reorganization plan did not explain the reasons for separating immigration inspection and border patrol functions from other immigration-related enforcement activities, which was contrary to the single Bureau of Border Security as prescribed by the Congress in the section 441 of the Homeland Security Act of 2002.

(8) Two years after this structure has been in effect, questions remain about whether the Department has organized itself properly, and is managing its customs and immigration enforcement and border security resources in the most efficient, sensible, and effective manner.

(9) The current structure has resulted in less cooperation and information sharing between these two critical functions than is desirable, and has caused operational and administrative difficulties that are hampering efforts to secure our borders and ensure the integrity of our border control system.

(10) United States Immigration and Customs Enforcement has faced major budgetary challenges that are, in part, attributable to the inexact division of resources upon the separation of immigration functions. These budget shortfalls have forced United States Immigration and Customs Enforcement to impose hiring freezes and to release aliens that otherwise should be detained.

(11) The current structure also has resulted in unnecessary overlap and duplication between United States Immigration and Customs Enforcement and United States Customs and Border Protection, both in the field and at the headquarters level. There are intelligence, legislative affairs, public affairs, and international affairs offices in both agencies.

(12) Border security and customs and immigration enforcement should be one seamless mission.

(b) REPORT.—

(1) IN GENERAL.—Not later than 30 days after the date of the enactment of this Act, the Secretary of Homeland Security shall review and evaluate the current organizational structure of the Department of Homeland Security established by the President's January 30, 2003, reorganization plan and submit a report of findings and recommendations to the Congress.

(2) CONTENTS OF REPORT.—The report shall include—

(A) a description of the rationale for, and any benefits of, the current organizational division of United States Immigration and Customs Enforcement and United States Customs and Border Protection, with respect to the Department's immigration and customs missions;

(B) a description of the organization, missions, operations, and policies of United States Customs and Border Protection and United States Immigration and Customs Enforcement, and areas of unnecessary overlap or operational gaps among and between these missions;

(C) an analysis of alternative organizational structures that could provide a more effective way to deliver maximum efficiencies and mission success;

(D) a description of the current role of the Directorate of Border and Transportation Security with respect to providing adequate direction and oversight of the two agencies, and whether this management structure is still necessary;

(E) an analysis of whether the Federal Air Marshals and the Federal Protective Service are properly located within the Department within United States Immigration and Customs Enforcement;

(F) the proper placement and functions of a specialized investigative and patrol unit operating at the southwest border on the Tohono O'odham Nation, known as the Shadow Wolves;

(G) the potential costs of reorganization, including financial, programmatic, and other costs, to the Department; and

(H) recommendations for correcting the operational and administrative problems that have been caused by the division of United States Customs

and Border Protection and United States Immigration and Customs Enforcement, including any appropriate reorganization plans.

SEC. 402. GAO REPORTS TO CONGRESS.

(a) IN GENERAL.— Not later than 6 months after the date of the enactment of this Act, the Comptroller General of the United States shall submit to the Congress a report that sets forth—

(1) an assessment of the effectiveness of the organizational and management structure of the Department of Homeland Security in meeting the Department's missions; and

(2) recommendations to facilitate and improve the organization and management of the Department to best meet those missions.

(b) CYBERSECURITY ASSESSMENT.—Not later than 6 months after the date of enactment of this Act, the Comptroller General shall submit a report to the Committees on Homeland Security and Energy and Commerce of the House of Representatives and the Committees on Homeland Security and Governmental Affairs and Commerce, Science, and Transportation of the Senate that sets forth an assessment of the effectiveness of the efforts of the Assistant Secretary for Cybersecurity to fulfill the statutory responsibilities of that office.

SEC. 403. PLAN FOR ESTABLISHING CONSOLIDATED AND COLOCATED REGIONAL OFFICES.

Not later than 60 days after the date of the enactment of this Act, the Secretary of Homeland Security shall develop and submit to the Congress a plan for establishing consolidated and colocated regional offices for the Department of Homeland Security in accordance with section 706 of the Homeland Security Act of 2002 (6 U.S.C. 346).

SEC. 404. PLAN TO REDUCE WAIT TIMES.

Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security shall develop a plan—

(1) to improve the operational efficiency of security screening checkpoints at commercial service airports so that average peak waiting periods at such checkpoints do not exceed 20 minutes; and

(2) to ensure that there are no significant disparities in immigration and customs processing times among airports that serve as international gateways.

SEC. 405. DENIAL OF TRANSPORTATION SECURITY CARD.

Section 70105(c) of title 46, United States Code, is amended—

(1) in paragraph (3) by inserting before the period "before an administrative law judge"; and

(2) by adding at the end the following:

"(5) In making a determination under paragraph (1)(D), the Secretary shall not consider a felony conviction if—

"(A) that felony occurred more than 7 years prior to the date of the Secretary's determination; and

"(B) the felony was not related to terrorism (as that term is defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)).".

SEC. 406. TRANSFER OF EXISTING CUSTOMS PATROL OFFICERS UNIT AND ESTABLISHMENT OF NEW CPO UNITS IN THE BUREAU OF IMMIGRATION AND CUSTOMS ENFORCEMENT.

(a) TRANSFER OF EXISTING UNIT.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall transfer to the Bureau of Immigration and Customs Enforcement all functions (including the personnel, assets, and obligations held by or available in connection with such functions) of the Customs Patrol Officers unit of the Bureau of Customs and Border Protection operating on the Tohono O'odham Indian reservation (commonly known as the 'Shadow Wolves' unit).

(b) ESTABLISHMENT OF NEW UNITS.—The Secretary is authorized to establish within the Bureau of Immigration and Customs Enforcement additional units of Customs Patrol Officers in accordance with this section.

(c) DUTIES.—The Secretary is authorized to establish within the Bureau of Immigration and Customs Enforcement additional units of Customs Patrol Officers in accordance with this section.

(d) BASIC PAY FOR JOURNEYMAN OFFICERS.—The rate of basic pay for a journeyman Customs Patrol Officer in a unit described in this section shall be not less than the rate of basic pay for GS–13 of the General Schedule.

(e) SUPERVISORS.—Each unit described under this section shall be supervised by a Chief Customs Patrol Officer, who shall have the same rank as a resident agent-in-charge of the Office of Investigations.

SEC. 407. AUTHORITY AND RESPONSIBILITY OF OTHER FEDERAL AGENCIES.

Nothing in this Act shall diminish or otherwise affect the authority or responsibility under statute, regulation, or Executive order of other Federal agencies than the Department of Homeland Security, including the Department of Commerce, the Department of Energy, the Department of Transportation, the Federal Communications Commission, the Nuclear Regulatory Commission, the Federal Energy Regulatory Commission, the Environmental Protection Agency, the Federal Trade Commission, and the National Telecommunications and Information Administration.

PURPOSE AND SUMMARY

The purpose of H.R. 1817, "Department of Homeland Security Authorization Act for Fiscal Year 2006," is to authorize appropriations for fiscal year 2006 for the Department of Homeland Security, and for other purposes.

BACKGROUND AND NEED FOR LEGISLATION

Our nation's critical infrastructure encompasses public and private facilities in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Computers are their nervous system. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, and switches that monitor and allow the nation's critical infrastructure to work. Thus, the healthy functioning of cyberspace is essential to the country's economic strength and its national security.

The issue of cybersecurity falls squarely within the jurisdiction of the Committee on Energy and Commerce. It is the Committee on Energy and Commerce that has cybersecurity jurisdiction due to its existing oversight of the networks, systems, facilities, and equipment over which any cybersecurity attack would occur and the potential effects of cybersecurity incidents on our nation's interstate and foreign commerce. When the House passed the Rules package for the 109th Congress, it did not contain language in Rule X granting the Committee on Homeland Security jurisdiction over cybersecurity issues. Importantly, language that would have given the Committee on Homeland Security some jurisdiction over cybersecurity was removed. Removal of this language was agreed to by the Republican Conference and later by a vote of the full House. The vote of the Republican Conference, and the vote adopting the Rules of the House, indicates that the Committee on Homeland Security is not the Committee of jurisdiction over issues involving cybersecurity.

Cybersecurity and the protection of critical infrastructure are both core parts of the jurisdiction of the Committee on Energy and Commerce. As the Committee with oversight of key critical infrastructure and the regulation of such infrastructure by agencies including the Department of Commerce, Department of Energy, Department of Transportation, Federal Communications Commission, Federal Trade Commission, Federal Energy Regulatory Commission, Nuclear Regulatory Commission, National Telecommunications and Information Administration, and the Environmental Protection Agency, the Committee is cognizant of the wide range of security protections each agency of expertise has implemented or is actively developing. For that reason, the Committee adopted a

Manager's amendment protecting the role of Federal agencies. Many of these agencies are taking steps to protect the critical infrastructure they regulate as well as their cyber assets. Additionally, the amendment makes clear that nothing in H.R. 1817 diminishes or alters the role of these Federal agencies as they actively work to protect the nation's critical infrastructure, both physical and cyber. H.R. 1817 does nothing to undermine the authority of federal agencies of expertise to require that industries for which they have responsibility meet existing and future prescribed security and safety requirements.

While the Committee would rather have had more time to hold hearings and mark up legislation addressing these issues, the Committee is responding to the tight time-limited referral of H.R. 1817. The Committee has jurisdiction over broad and far-reaching subjects, including telecommunications, energy, health care, the environment, commerce, trade, and consumer protection. Due to time constraints, however, there were issues in H.R. 1817 that the Committee did not address, but that was not for lack of Committee jurisdiction. While H.R. 1817, as reported by the Committee on Energy and Commerce, addresses only some concerns relating to the Committee's jurisdiction, the Committee intends to return to these issues later in the year in a more comprehensive fashion.

H.R. 1817 establishes a myriad of new programs and offices, a number of whose functions fall within this Committee's jurisdiction. Chief among them are sections 311–314, that among other things, create a new Assistant Secretary for Cybersecurity within the Department of Homeland Security. Section 313 defines "cybersecurity." Further, in sections 331–333, the bill requires the Department of Homeland Security to create a prioritization plan and complete a security review on how to protect the nation's "critical infrastructure." Critical infrastructure encompasses many assets, including information, telecommunications, energy, financial services, water, and transportation networks and facilities. Such critical infrastructure assets are crucial to the country's interstate and foreign commerce and national security.

The Committee has strong concerns about duplicative regulatory and oversight regimes and the impact they could have on interstate and foreign commerce as well as national security. The bill includes provisions that appear to grant the Department of Homeland Security (DHS) authority that overlaps with the responsibilities of other agencies within the jurisdiction of the Energy and Commerce Committee. Depending on future interpretation of these provisions, the result could be inconsistent oversight or regulation of various industries that already are responding to terrorism or other security directives from the agencies with direct regulatory authority over them. There is a risk that redundant, competing, and possibly conflicting obligations or priorities could be imposed upon businesses, such as the electric transmission, nuclear power, or telecommunications industries. It is unclear whether the nation's safety and security would be enhanced by such dual authority, or whether the related expenditure of federal funds would be warranted. In addition, dual oversight or regulation could blur lines of accountability, both within government and industry.

HEARINGS

No hearings on this legislation have yet been held in the 109th Congress.

COMMITTEE CONSIDERATION

On Wednesday, May 11, 2005, the Full Committee met in open markup session and ordered H.R. 1817 favorably reported to the House, as amended, by a voice vote, a quorum being present.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto. There were no record votes taken in connection with ordering H.R. 1817 reported. A motion by Chairman Barton to order H.R. 1817 reported to the House, as amended, was agreed to by a voice vote.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee did not hold any hearings on this legislation in the 109th Congress.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

The purpose of H.R. 1817, the Department of Homeland Security Authorization Act for FY 2006, is to authorize appropriations for fiscal year 2006 for the Department of Homeland Security, and for other purposes.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 1817, the "Department of Homeland Security Authorization Act for Fiscal Year 2006," would result in changes to budget authority, entitlement authority, and tax expenditures and revenues to the extent stated below in the Committee Cost Estimate.

COMMITTEE COST ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, May 13, 2005.

Hon. JOE BARTON,
Chairman, Committee on Energy and Commerce,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 1817, the Department of Homeland Security Authorization Act for Fiscal Year 2006.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Mark Grabowicz (for federal costs), and Melissa Merrell (for the impact on state and local governments).

Sincerely,

(For Douglas Holtz-Eakin, Director).

Enclosure.

H.R. 1817—Department of Homeland Security Authorization Act for Fiscal Year 2006

Summary: H.R 1817 would authorize the appropriation of $34.2 billion for fiscal year 2006 to fund the major operations of the Department of Homeland Security (DHS). CBO estimates that, implementing H.R. 1817 would cost about $33 billion over the 2006–2010 period, assuming appropriation of the authorized amounts. Enacting the bill would not affect direct spending or receipts.

H.R. 1817 contains an intergovmental mandate as defined in the Unfunded Mandates Reform Act (UMRA) by exempting certain information related to critical infrastructure from state and local laws that provide public access to information. CBO estimates that the costs, if any, to state and local governments would be minimal and well below the annual threshold established in that act ($62 million in 2005, adjusted annually for inflation). H.R. 1817 . contains no new private-sector mandates as defined in UMRA.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 1817 is shown in the following table. For this estimate, CBO assumes that the authorized amounts will be appropriated near the beginning of fiscal year 2006 and that outlays will follow the historical spending rates. for these activities. The costs of this legislation fall within budget functions 050 (national defense), 300 (natural resources and environment), 400 (transportation), 450 (community and regional development), 550 (health), 600 (income security), 750 (administration of justice), and 800 (general government).

	By fiscal year, in millions of dollars—					
	2005	2006	2007	2008	2009	2010
SPENDING SUBJECT TO APPROPRIATION						
Department of Homeland Security:						
Spending Under Current Law:						
Estimated Budget Authority[a]	38,469	0	0	0	0	0
Estimated Outlays	31,928	14,443	7,939	3,475	1,308	594
Proposed Changes:						
Authorization Level	0	34,152	0	0	0	0
Estimated Outlays	0	17,418	7,513	5,123	2,391	683

	By fiscal year, in millions of dollars—					
	2005	2006	2007	2008	2009	2010
Department of Homeland Security:						
Spending Under H.R. 1817:						
Estimated Budget Authority[a]	38,469	34,152	0	0	0	0
Estimated Outlays	31,928	31,861	15,452	8,598	3,699	1,277

[a] The estimated 2005 level is the amount of appropriations less offsetting collections for that year for operations of DHS.

Intergovernmental and private-sector impact: H.R. 1817 contains an intergovernmental mandate as defined in UMRA by exempting certain information related to critical infrastructure from state and local laws that provide public access to information. CBO estimates that the costs, if any to state and local governments would be minimal and well below the annual threshold established in that act ($62 million in 2005, adjusted annually for inflation). H.R. 1817 contains no new private-sector mandates as defined in UMRA.

Section 306 would require the Secretary of the Department of Homeland Security to issue regulations for the security of maritime cargo moving within the intermodal transportation system. Those regulations would relate to the securing, recording, and verifying of seals on maritime cargo containers in the hauling of cargo from one mode of transportation to another. According to DHS, a notice of proposed rulemaking that incorporates the recommendations referred to in the bill has been drafted and is pending review. Based on information from DHS, CBO anticipates that the Secretary will issue those regulations. Thus, CBO expects that the provisions this section would impose no additional mandates on public or private-sector entities. State and local governments would benefit from programs to improve interoperable communications and to reimburse costs for having law enforcement officers trained to enforce immigration laws. Any costs incurred by those governments would be incurred voluntarily.

Previous CBO estimates: On May 6, 2005, CBO transmitted a cost estimate for H.R. 1817 as ordered reported by the House Committee on Homeland Security on April 27, 2005. On May 13, 2005, CBO transmitted a cost estimate for H.R. 1817 as ordered reported by the House Committee on the Judiciary on May 12, 2005. The three versions of the bill are similar, and all three cost estimates are identical.

Estimate prepared by: federal costs: Mark Grabowicz; impact on state, local, and tribal governments; Melissa Merrell; impact on the private sector: Paige Piper/Bach.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 3, which grants Congress the power to regulate commerce with foreign nations, among the several States, and with the Indian tribes.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

The section-by-section contained in this report reflects the amendments that were adopted during the Committee on Energy and Commerce markup of H.R. 1817, as reported by the Committee on Homeland Security. Due to the time constraints imposed on the Committee to report H.R. 1817, the section-by-section reflects only the amendments that were adopted during the Full Committee markup. The fact that the Committee did not undertake amendments on other aspects of H.R. 1817 should not be construed as a waiver of the Committee on Energy and Commerce's jurisdiction over other provisions of this bill. A complete section-by-section to H.R. 1817, as reported by the Committee on Homeland Security, can be found in House Report 109–71, Part I. The Committee on Energy and Commerce takes no position on the contents of the section-by-section of the Committee on Homeland Security report on H.R. 1817.

Section 109. Metropolitan Medical Response System

Section 109 authorizes the Metropolitan Medical Response System for fiscal year 2006 at $75 million of the total authorized under section 101.

Section 302. Technology development and transfer

Subsection (c) requires the Department to report to the Committees on Homeland Security and Energy and Commerce of the House of Representatives and the Committees on Homeland Security and Governmental Affairs and Commerce, Science, and Transportation of the Senate on its status in implementing the functions of the Technology Clearinghouse, as well as the S&T Directorate's progress in reviewing unsolicited technology proposals.

Section 306. Security of maritime cargo containers

Section 306(c)(2) and 306(d)(3) requires the Secretary to submit reports to the Committees on Homeland Security and Energy and Commerce of the House of Representatives and the Committees on Homeland Security and Governmental Affairs and Commerce, Science, and Transportation of the Senate on the implementation of those sections.

Section 312. Assistant Secretary for Cybersecurity

Section 312(a) establishes the position of Assistant Secretary for Cybersecurity that will be appointed by the President. Section 312(b) specifies the Assistant Secretary for Cybersecurity will have responsibility for the National Cyber Security Division and the National Communications System within DHS. Additionally, section 312(b) lists the Assistant Secretary's responsibilities. These responsibilities are certain cybersecurity-related duties currently assigned to the Under Secretary for Information Analysis and Infrastructure Protection under 6 U.S.C. 201. Specifically, the new Assistant Secretary will be responsible for cybersecurity-related duties in subsections (2), (3), (5), (6), (15), and (17) of section 201(d) of the Homeland Security Act of 2002. The legislation creates no new cybersecurity-related authority for either the Assistant Secretary or the Department.

Section 312(c) requires the Assistant Secretary for Cybersecurity to coordinate all activities under this subtitle with other Federal agencies, including the Department of Commerce, Department of Energy, Department of Transportation, Federal Communications Commission, Federal Trade Commission, Nuclear Regulatory Commission, Federal Energy Regulatory Commission, National Telecommunications and Information Administration, and the Environmental Protection Agency.

Because these agencies of expertise are developing and implementing cybersecurity priorities and measures to protect their own infrastructure, as well as creating policies and practices for their regulated industries, it is vitally important to maintain coordination with these relevant Federal agencies.

An area of importance to the Committee is the creation of cybersecurity best practices. The Network Reliability and Interoperability Council (NRIC) and the Media Security and Reliability Council, two Federal advisory committees overseen by the Federal Communications Commission, have undertaken initiatives to protect communications infrastructure. The Homeland Defense Group was initially chartered by NRIC VI in March 2002 to focus on the development of best practices to prevent disruptions of public telecommunications services and the Internet to effectively restore those services and facilities in the event of disruption. This entailed studying and developing hundreds of best practices relating to cybersecurity. These efforts were continued in the charter for NRIC VII. Those best practices were recently reviewed by NRIC to determine if any gaps exist between NRIC best practices and existing industry best practices for cybersecurity. A final report is due by December 16, 2005. Recently Federal Communications Commission officials have been conducting on-site seminars across the country to help implement NRIC's best practices throughout the communications industry. The Assistant Secretary for Cybersecurity shall coordinate with NRIC and other Federal agencies. As a result of the changes made by the Committee, section 315 of the bill, as reported by the Committee on Homeland Security, was deleted.

Section 313. Cybersecurity defined

Section 313 defines for the term "cybersecurity" for purposes of subtitle B. The term "cybersecurity" is defined as the protection and restoration of networked electronic equipment and facilities,

including hardware and software and the information contained therein, from intrusion, interference, and incapacitation."

Section 331. Critical infrastructure

Section 331 requires the Secretary of Homeland Security to complete the prioritization of critical infrastructure no later than 90 days after enactment according to the following criteria: the threat of terrorist attack, based on information received by the DHS Office of Information Analysis regarding the intentions and capabilities of terrorist groups and other potential threats; the likelihood that an attack would cause the disruption of such infrastructure; and the likelihood that such an attack would result in substantial numbers of human deaths and serious bodily injuries, a substantial adverse impact on the national economy, or a significant adverse impact on the national security.

Section 331(b) requires the Secretary to coordinate the prioritization under this section with other Federal agencies of expertise, including the Department of Commerce, Department of Energy, Department of Transportation, Federal Communications Commission, Federal Trade Commission, Nuclear Regulatory Commission, Federal Energy Regulatory Commission, National Telecommunications and Information Administration, and the Environmental Protection Agency.

Section 332. Security review

Section 332(a) requires the Secretary of DHS to review existing security plans for securing the specific facilities included in the prioritized list, to recommend changes to existing security plans, and to coordinate and contribute to critical infrastructure protective efforts of Federal, State, and local agencies and the private sector as set out in Homeland Security Presidential Directive 7 (HSPD–7, Dec. 17, 2003). Recommendations for security plans made under this section shall include protective measures to secure such infrastructure, and milestones and timeframes for implementation. Section 332(c) requires the Secretary to coordinate the security review and recommendations under this section with other Federal agencies of expertise, including the Department of Commerce, Department of Energy, Department of Transportation, Federal Communications Commission, Federal Trade Commission, Nuclear Regulatory Commission, Federal Energy Regulatory Commission, National Telecommunications and Information Administration, and the Environmental Protection Agency.

Section 333. Implementation report

Section 333(a) directs the Secretary of Homeland Security to report on the implementation of this subtitle to the Committees on Homeland Security and Energy and Commerce of the House of Representatives and the Committees on Homeland Security and Governmental Affairs and Commerce, Science, and Transportation of the Senate no later than 15 months after enactment of this Act. Following the coordination required by section 332(c), section 333(b) requires the Secretary to provide an updated report to the Committees on Homeland Security and Energy and Commerce of the House of Representatives and the Committees on Homeland Security and Governmental Affairs and Commerce, Science, and

Transportation of the Senate not later than one year after the first report.

Section 402. GAO report to Congress

Section 402(a) requires the Government Accountability Office (GAO) to submit a report to Congress on the effectiveness of the organizational and management structure of DHS in meeting its missions with recommendations to facilitate and improve organization and management of the Department. The Committee expects to receive a copy of this report.

Section 402(b) requires the GAO, not later than 6 months after the enactment of this act, to submit a report to the Committees on Homeland Security and Energy and Commerce of the House of Representatives and the Committees on Homeland Security and Governmental Affairs and Commerce, Science, and Transportation of the Senate on the effectiveness of the efforts of the Assistant Secretary for Cybersecurity to fulfill the statutory responsibilities of that office.

Section 407. Authority and responsibility of other federal agencies

Section 407 states that nothing in this Act shall diminish or otherwise affect the authority or responsibility under statute, regulation, or Executive order of Federal agencies other than the DHS. Thus, this Act does nothing to undermine the authority of federal agencies of expertise to require that industries for which they have responsibility meet existing and future prescribed security and safety requirements.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

* * * * * * *

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) * * *

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE I—DEPARTMENT OF HOMELAND SECURITY

* * * * * * *

SEC. 102. SECRETARY; FUNCTIONS.

(a) * * *

* * * * * * *

(e) PARTICIPATION IN FOREIGN COLLECTION REQUIREMENTS AND MANAGEMENT PROCESSES.—The Secretary shall be a member of any Federal Government interagency board, established by Executive order or any other binding interagency directive, that is responsible for establishing foreign collection information requirements and priorities for estimative analysis.

[(e)**]** *(f)* ISSUANCE OF REGULATIONS.—The issuance of regulations by the Secretary shall be governed by the provisions of chapter 5 of title 5, United States Code, except as specifically provided in this Act, in laws granting regulatory authorities that are transferred by this Act, and in laws enacted after the date of enactment of this Act.

[(f)**]** *(g)* SPECIAL ASSISTANT TO THE SECRETARY.—The Secretary shall appoint a Special Assistant to the Secretary who shall be responsible for—

(1) * * *

* * * * * * *

[(g)**]** *(h)* STANDARDS POLICY.—All standards activities of the Department shall be conducted in accordance with section 12(d) of the National Technology Transfer Advancement Act of 1995 (15 U.S.C. 272 note) and Office of Management and Budget Circular A–119.

* * * * * * *

SEC. 104. AUTHORITY FOR DISSEMINATING HOMELAND SECURITY INFORMATION.

(a) PRIMARY AUTHORITY.—Except as provided in subsection (b), the Secretary shall be the executive branch official responsible for disseminating homeland security information to State and local government and tribal officials and the private sector.

(b) PRIOR APPROVAL REQUIRED.—No Federal official may disseminate any homeland security information, as defined in section

892(f)(1), to State, local, tribal, or private sector officials without the Secretary's prior approval, except—

(1) in exigent circumstances under which it is essential that the information be communicated immediately; or

(2) when such information is issued to State, local, or tribal law enforcement officials for the purpose of assisting them in any aspect of the administration of criminal justice.

SEC. 105. HOMELAND SECURITY INFORMATION REQUIREMENTS BOARD.

(a) ESTABLISHMENT OF BOARD.—There is established an interagency Homeland Security Information Requirements Board (hereinafter in this section referred to as the "Information Requirements Board").

(b) MEMBERSHIP.—The following officials are members of the Information Requirements Board:

(1) The Secretary of Homeland Security, who shall serve as the Chairman of the Information Requirements Board.

(2) The Attorney General.

(3) The Secretary of Commerce.

(4) The Secretary of the Treasury.

(5) The Secretary of Defense.

(6) The Secretary of Energy.

(7) The Secretary of State.

(8) The Secretary of the Interior.

(9) The Director of National Intelligence.

(10) The Director of the Federal Bureau of Investigation.

(11) The Director of the National Counterterrorism Center.

(12) The Chief Privacy Officer of the Department of Homeland Security.

(c) FUNCTIONS.—

(1) OVERSIGHT OF HOMELAND SECURITY REQUIREMENTS.—The Information Requirements Board shall oversee the process for establishing homeland security requirements and collection management for all terrorism-related information and all other homeland security information (as defined in section 892(f)(1)) collected within the United States.

(2) DETERMINATION OF COLLECTION PRIORITIES.—The Information Requirements Board shall—

(A) determine the domestic information collection requirements for information relevant to the homeland security mission; and

(B) prioritize the collection and use of such information.

(3) COORDINATION OF COLLECTION REQUIREMENTS AND MANAGEMENT ACTIVITIES.—

(A) COORDINATION WITH COUNTERPART AGENCIES.—The Chairman shall ensure that the Information Requirements Board carries out its activities in a manner that is fully coordinated with the Board's counterpart entities.

(B) PARTICIPATION OF COUNTERPART ENTITIES.—The Chairman and the Director of National Intelligence shall ensure that each counterpart entity—

(i) has at least one representative on the Information Requirement Board and on every subcomponent of the Board; and

(ii) meets jointly with the Information Requirements Board (and, as appropriate, with any subcomponent of the Board) as often as the Chairman and the Director of National Intelligence determine appropriate.

(C) COUNTERPART ENTITY DEFINED.—In this section, the term "counterpart entity" means an entity of the Federal Government that is responsible for foreign intelligence collection requirements and management.

(d) MEETINGS.—

(1) IN GENERAL.—The Information Requirements Board shall meet regularly at such times and places as its Chairman may direct.

(2) INVITED REPRESENTATIVES.—The Chairman may invite representatives of Federal agencies not specified in subsection (b) to attend meetings of the Information Requirements Board.

TITLE II—INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION

Subtitle A—Directorate for Information Analysis and Infrastructure Protection; Access to Information

SEC. 201. DIRECTORATE FOR INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION.

(a) * * *

(b) ASSISTANT SECRETARY FOR INFORMATION ANALYSIS; ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION.—

(1) * * *

* * * * * * *

(3) ASSISTANT SECRETARY FOR CYBERSECURITY.—There shall be in the Department an Assistant Secretary for Cybersecurity, who shall be appointed by the President.

[(3)**]** *(4)* RESPONSIBILITIES.—The Assistant Secretary for Information **[**Analysis and the**]** *Analysis, the* Assistant Secretary for Infrastructure **[**Protection shall**]** *Protection, and the Assistant Secretary for Cybersecurity shall* assist the Under Secretary for Information Analysis and Infrastructure Protection in discharging the responsibilities of the Under Secretary under this section.

* * * * * * *

(d) RESPONSIBILITIES OF UNDER SECRETARY.—Subject to the direction and control of the Secretary, the responsibilities of the Under Secretary for Information Analysis and Infrastructure Protection shall be as follows:

(1) * * *

* * * * * * *

(7) To administer the Homeland Security Advisory System *under section 205*, including—

(A) * * *

* * * * * * *

(20) To require, in consultation with the Assistant Secretary for Infrastructure Protection, the creation and routine dissemination of analytic reports and products designed to provide timely and accurate information that has specific relevance to each of the Nation's critical infrastructure sectors (as identified in the national infrastructure protection plan issued under paragraph (5)), to private sector officials in each such sector who are responsible for protecting institutions within that sector from potential acts of terrorism and for mitigating the potential consequences of any such act.

(21) To ensure sufficient analytic expertise within the Office of Information Analysis to create and disseminate, on an ongoing basis, products based on the analysis of homeland security information, as defined in section 892(f)(1), with specific reference to the threat of terrorism involving the use of nuclear weapons and biological agents to inflict mass casualties or other catastrophic consequences on the population or territory of the United States.

(22) To ensure that—

(A) the Assistant Secretary for Information Analysis receives promptly and without request all information obtained by any component of the Department if that information relates, directly or indirectly, to a threat of terrorism involving the potential use of nuclear weapons;

(B) such information is—

(i) integrated and analyzed comprehensively; and

(ii) disseminated in a timely manner, including to appropriately cleared State, local, tribal, and private sector officials; and

(C) such information is used to determine what requests the Department should submit for collection of additional information relating to that threat.

(23) To ensure that the Assistant Secretary for Information Analysis—

(A) is routinely and without request given prompt access to all terrorism-related information collected by or otherwise in the possession of any component of the Department, including all homeland security information (as that term is defined in section 892(f)(1)); and

(B) to the extent technologically feasible has direct access to all databases of any component of the Department that may contain such information.

(24) To administer the homeland security information network, including—

(A) exercising primary responsibility for establishing a secure nationwide real-time homeland security information sharing network for Federal, State, and local government agencies and authorities, tribal officials, the private sector, and other governmental and private entities involved in receiving, analyzing, and distributing information related to threats to homeland security;

(B) ensuring that the information sharing systems, developed in connection with the network established under subparagraph (A), are utilized and are compatible with, to the greatest extent practicable, Federal, State, and local govern-

ment, tribal, and private sector antiterrorism systems and protocols that have been or are being developed; and

(C) ensuring, to the greatest extent possible, that the homeland security information network and information systems are integrated and interoperable with existing private sector technologies.

(25) To ensure that, whenever possible—

(A) the Assistant Secretary for Information Analysis produces and disseminates reports and analytic products based on open-source information that do not require a national security classification under applicable law; and

(B) such unclassified open-source reports are produced and disseminated contemporaneously with reports or analytic products concerning the same or similar information that the Assistant Secretary for Information Analysis produces and disseminates in a classified format.

* * * * * * *

SEC. 203. ALTERNATIVE ANALYSIS OF HOMELAND SECURITY INFORMATION.

The Secretary shall establish a process and assign an individual or entity the responsibility to ensure that, as appropriate, elements of the Department conduct alternative analysis (commonly referred to as "red-team analysis") of homeland security information, as that term is defined in section 892(f)(1), that relates to potential acts of terrorism involving the use of nuclear weapons or biological agents to inflict mass casualties or other catastrophic consequences on the population or territory of the United States.

SEC. 204. 9/11 MEMORIAL HOMELAND SECURITY FELLOWS PROGRAM.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Secretary shall establish a fellowship program in accordance with this section for the purpose of bringing State, local, tribal, and private sector officials to participate in the work of the Homeland Security Operations Center in order to become familiar with—

(A) the mission and capabilities of that Center; and

(B) the role, programs, products, and personnel of the Office of Information Analysis, the Office of Infrastructure Protection, and other elements of the Department responsible for the integration, analysis, and dissemination of homeland security information, as defined in section 892(f)(1).

(2) PROGRAM NAME.—The program under this section shall be known as the 9/11 Memorial Homeland Security Fellows Program.

(b) ELIGIBILITY.—In order to be eligible for selection as a fellow under the program, an individual must—

(1) have homeland security-related responsibilities; and

(2) possess an appropriate national security clearance.

(c) LIMITATIONS.—The Secretary—

(1) may conduct up to 4 iterations of the program each year, each of which shall be 90 days in duration; and

(2) shall ensure that the number of fellows selected for each iteration does not impede the activities of the Center.

(d) CONDITION.—As a condition of selecting an individual as a fellow under the program, the Secretary shall require that the individual's employer agree to continue to pay the individual's salary and benefits during the period of the fellowship.

(e) STIPEND.—During the period of the fellowship of an individual under the program, the Secretary shall, subject to the availability of appropriations—

(1) provide to the individual a stipend to cover the individual's reasonable living expenses during the period of the fellowship; and

(2) reimburse the individual for round-trip, economy fare travel to and from the individual's place of residence twice each month.

SEC. 205. HOMELAND SECURITY ADVISORY SYSTEM.

(a) REQUIREMENT.—The Under Secretary for Information Analysis and Infrastructure Protection shall implement a Homeland Security Advisory System in accordance with this section to provide public advisories and alerts regarding threats to homeland security, including national, regional, local, and economic sector advisories and alerts, as appropriate.

(b) REQUIRED ELEMENTS.—The Under Secretary, under the System—

(1) shall include, in each advisory and alert regarding a threat, information on appropriate protective measures and countermeasures that may be taken in response to the threat;

(2) shall, whenever possible, limit the scope of each advisory and alert to a specific region, locality, or economic sector believed to be at risk; and

(3) shall not, in issuing any advisory or alert, use color designations as the exclusive means of specifying the homeland security threat conditions that are the subject of the advisory or alert.

SEC. 206. FULL AND EFFICIENT USE OF OPEN-SOURCE INFORMATION.

The Under Secretary shall ensure that, in meeting their analytic responsibilities under section 201(d) and in formulating requirements for collection of additional information, the Assistant Secretary for Information Analysis and the Assistant Secretary for Infrastructure Protection make full and efficient use of open-source information wherever possible.

* * * * * * *

TITLE III—SCIENCE AND TECHNOLOGY IN SUPPORT OF HOMELAND SECURITY

* * * * * * *

SEC. 313. TECHNOLOGY CLEARINGHOUSE TO ENCOURAGE AND SUPPORT INNOVATIVE SOLUTIONS TO ENHANCE HOMELAND SECURITY.

(a) * * *

(b) ELEMENTS OF PROGRAM.—The program described in subsection (a) shall include the following components:

(1) * * *

* * * * * * *

(6) The establishment of a homeland security technology transfer program to facilitate the identification, modification, and commercialization of technology and equipment for use by Federal, State, and local governmental agencies, emergency response providers, and the private sector to prevent, prepare for, or respond to acts of terrorism.

(c) TECHNOLOGY TRANSFER PROGRAM.—In developing the program described in subsection (b)(6), the Secretary, acting through the Under Secretary for Science and Technology, shall—

(1) in consultation with the other Under Secretaries of the Department and the Director of the Office for Domestic Preparedness, on an ongoing basis—

(A) conduct surveys and reviews of available appropriate technologies that have been, or are in the process of being developed, tested, evaluated, or demonstrated by the Department, other Federal agencies, or the private sector or foreign governments and international organizations and that may be useful in assisting Federal, State, and local governmental agencies, emergency response providers, or the private sector to prevent, prepare for, or respond to acts of terrorism;

(B) conduct or support research, development, tests, and evaluations, as appropriate of technologies identified under subparagraph (A), including any necessary modifications to such technologies for antiterrorism use;

(C) communicate to Federal, State, and local governmental agencies, emergency response providers, or the private sector the availability of such technologies for antiterrorism use, as well as the technology's specifications, satisfaction of appropriate standards, and the appropriate grants available from the Department to purchase such technologies;

(D) coordinate the selection and administration of all technology transfer activities of the Science and Technology Directorate, including projects and grants awarded to the private sector and academia; and

(E) identify priorities based on current risk assessments within the Department of Homeland Security for identifying, researching, developing, testing, evaluating, modifying, and fielding existing technologies for antiterrorism purposes;

(2) in support of the activities described in paragraph (1)—

(A) consult with Federal, State, and local emergency response providers;

(B) consult with government agencies and nationally recognized standards development organizations as appropriate;

(C) enter into agreements and coordinate with other Federal agencies, foreign governments, and national and international organizations as the Secretary determines appropriate, in order to maximize the effectiveness of such technologies or to facilitate commercialization of such technologies; and

(D) consult with existing technology transfer programs and Federal and State training centers that research, develop, test, evaluate, and transfer military and other technologies for use by emergency response providers; and

(3) establish a working group in coordination with the Secretary of Defense to advise and assist the technology clearinghouse in the identification of military technologies that are in the process of being developed, or are developed, by the Department of Defense or the private sector, which may include—

(A) representatives from the Department of Defense or retired military officers;

(B) nongovernmental organizations or private companies that are engaged in the research, development, testing, or evaluation of related technologies or that have demonstrated prior experience and success in searching for and identifying technologies for Federal agencies;

(C) Federal, State, and local emergency response providers; and

(D) to the extent the Secretary considers appropriate, other organizations, other interested Federal, State, and local agencies, and other interested persons.

[(c)**]** *(d)* MISCELLANEOUS PROVISIONS.—

(1) * * *

* * * * * * *

TITLE IV—DIRECTORATE OF BORDER AND TRANSPORTATION SECURITY

* * * * * * *

Subtitle C—Miscellaneous Provisions

* * * * * * *

SEC. 430. OFFICE FOR DOMESTIC PREPAREDNESS.

(a) * * *

* * * * * * *

(c) RESPONSIBILITIES.—The Office for Domestic Preparedness shall have the primary responsibility within the executive branch of Government for the preparedness of the United States for acts of terrorism, including—

(1) * * *

* * * * * * *

(8) those elements of the Office of National Preparedness of the Federal Emergency Management Agency which relate to terrorism, which shall be consolidated within the Department in the Office for Domestic Preparedness established under this section; **[**and**]**

(9) helping to ensure the acquisition of interoperable communication technology by State and local governments and emergency response providers**[**.**]***; and*

(10) designing, developing, performing, and evaluating exercises at the national, State, territorial, regional, local, and trib-

al levels of government that incorporate government officials, emergency response providers, public safety agencies, the private sector, international governments and organizations, and other appropriate entities to test the Nation's capability to prevent, prepare for, respond to, and recover from threatened or actual acts of terrorism.

* * * * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * * * *

Subtitle J—Terrorism Preparedness Exercises

SEC. 899a. NATIONAL TERRORISM EXERCISE PROGRAM.

(a) IN GENERAL.—The Secretary, through the Office for Domestic Preparedness, shall establish a National Terrorism Exercise Program for the purpose of testing and evaluating the Nation's capabilities to prevent, prepare for, respond to, and recover from threatened or actual acts of terrorism that—

(1) enhances coordination for terrorism preparedness between all levels of government, emergency response providers, international governments and organizations, and the private sector;

(2) is—

(A) multidisciplinary in nature, including, as appropriate, information analysis and cybersecurity components;

(B) as realistic as practicable and based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(C) carried out with the minimum degree of notice to involved parties regarding the timing and details of such exercises, consistent with safety considerations;

(D) evaluated against performance measures and followed by corrective action to solve identified deficiencies; and

(E) assessed to learn best practices, which shall be shared with appropriate Federal, State, territorial, regional, local, and tribal personnel, authorities, and training institutions for emergency response providers; and

(3) assists State, territorial, local, and tribal governments with the design, implementation, and evaluation of exercises that—

(A) conform to the requirements of paragraph (2); and

(B) are consistent with any applicable State homeland security strategy or plan.

(b) NATIONAL LEVEL EXERCISES.—The Secretary, through the National Terrorism Exercise Program, shall perform on a periodic basis national terrorism preparedness exercises for the purposes of—

(1) involving top officials from Federal, State, territorial, local, tribal, and international governments, as the Secretary considers appropriate;

(2) testing and evaluating the Nation's capability to detect, disrupt, and prevent threatened or actual catastrophic acts of terrorism, especially those involving weapons of mass destruction; and

(3) testing and evaluating the Nation's readiness to respond to and recover from catastrophic acts of terrorism, especially those involving weapons of mass destruction.

(c) CONSULTATION WITH FIRST RESPONDERS.—In implementing the responsibilities described in subsections (a) and (b), the Secretary shall consult with a geographic (including urban and rural) and substantive cross section of governmental and nongovernmental first responder disciplines, including as appropriate—

(1) Federal, State, and local first responder training institutions;

(2) representatives of emergency response providers; and

(3) State and local officials with an expertise in terrorism preparedness.

* * * * * * *

TITLE 5, UNITED STATES CODE

* * * * * * *

PART III—EMPLOYEES

* * * * * * *

SUBPART I—MISCELLANEOUS

* * * * * * *

CHAPTER 97—DEPARTMENT OF HOMELAND SECURITY

Sec.
9701. Establishment of human resources management system.
9702. Recruitment bonuses.
9703. Reemployed annuitants.
9704. Regulations.

* * * * * * *

§ 9702. Recruitment bonuses

(a) IN GENERAL.—Notwithstanding any provision of chapter 57, the Secretary of Homeland Security, acting through the Under Secretary for Information Analysis and Infrastructure Protection, may pay a bonus to an individual in order to recruit such individual for a position that is primarily responsible for discharging the analytic responsibilities specified in section 201(d) of the Homeland Security Act of 2002 (6 U.S.C. 121(d)) and that—

(1) is within the Directorate for Information Analysis and Infrastructure Protection; and

(2) would be difficult to fill in the absence of such a bonus. In determining which individuals are to receive bonuses under this section, appropriate consideration shall be given to the Directorate's critical need for linguists.

(b) BONUS AMOUNT, FORM, ETC.—

(1) IN GENERAL.—The amount of a bonus under this section shall be determined under regulations of the Secretary of Homeland Security, but may not exceed 50 percent of the annual rate of basic pay of the position involved.

(2) FORM OF PAYMENT.—A bonus under this section shall be paid in the form of a lump-sum payment and shall not be considered to be part of basic pay.

(3) COMPUTATION RULE.—For purposes of paragraph (1), the annual rate of basic pay of a position does not include any comparability payment under section 5304 or any similar authority.

(c) SERVICE AGREEMENTS.—Payment of a bonus under this section shall be contingent upon the employee entering into a written service agreement with the Department of Homeland Security. The agreement shall include—

(1) the period of service the individual shall be required to complete in return for the bonus; and

(2) the conditions under which the agreement may be terminated before the agreed-upon service period has been completed, and the effect of any such termination.

(d) ELIGIBILITY.—A bonus under this section may not be paid to recruit an individual for—

(1) a position to which an individual is appointed by the President, by and with the advice and consent of the Senate;

(2) a position in the Senior Executive Service as a noncareer appointee (as defined under section 3132(a)); or

(3) a position which has been excepted from the competitive service by reason of its confidential, policy-determining, policy-making, or policy-advocating character.

(e) TERMINATION.—The authority to pay bonuses under this section shall terminate on September 30, 2008.

§ 9703. Reemployed annuitants

(a) IN GENERAL.—If an annuitant receiving an annuity from the Civil Service Retirement and Disability Fund becomes employed in a position within the Directorate for Information Analysis and Infrastructure Protection of the Department of Homeland Security, the annuitant's annuity shall continue. An annuitant so reemployed shall not be considered an employee for the purposes of chapter 83 or 84.

(b) TERMINATION.—The exclusion pursuant to this section of the Directorate for Information Analysis and Infrastructure Protection from the reemployed annuitant provisions of chapters 83 and 84 shall terminate 3 years after the date of the enactment of this section, unless extended by the Secretary of Homeland Security. Any such extension shall be for a period of 1 year and shall be renewable.

(c) ANNUITANT DEFINED.—For purposes of this section, the term "annuitant" has the meaning given such term under section 8331 or 8401, whichever is appropriate.

§ 9704. Regulations

The Secretary of Homeland Security, in consultation with the Director of the Office of Personnel Management, may prescribe any regulations necessary to carry out section 9702 or 9703.

* * * * * * *

SECTION 70105 OF TITLE 46, UNITED STATES CODE

§ 70105. Transportation security cards

(a) * * *

* * * * * * *

(c) DETERMINATION OF TERRORISM SECURITY RISK.—(1) * * *

* * * * * * *

(3) The Secretary shall establish an appeals process under this section for individuals found to be ineligible for a transportation security card that includes notice and an opportunity for a hearing *before an administrative law judge*.

* * * * * * *

(5) In making a determination under paragraph (1)(D), the Secretary shall not consider a felony conviction if—

(A) that felony occurred more than 7 years prior to the date of the Secretary's determination; and

(B) the felony was not related to terrorism (as that term is defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)).

* * * * * * *

○